Sicherheit von Location Based Services im Überblick

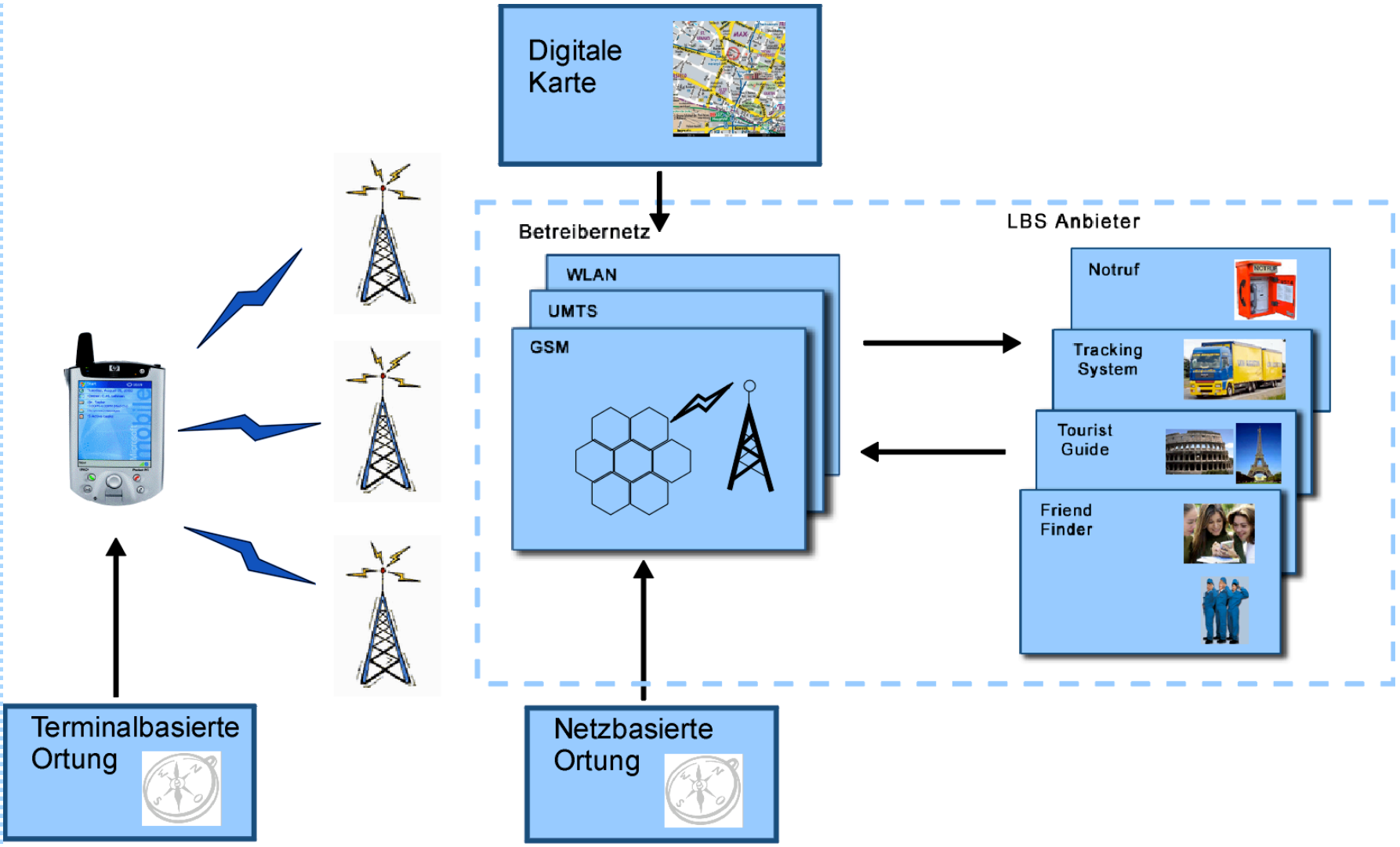
Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit
http://www-sec.uni-regensburg.de

Gliederung

- Einführung
- Rechtliche Anforderungen
- Positionsbestimmungsverfahren
- Standards und Protokolle
- Schlussbemerkungen

Standortbezogene Dienste (Location Based Services, LBS) sind über ein Netzwerk erbrachte mobile Dienste, die unter Zuhilfenahme von positions-, zeit- und nutzerabhängigen Daten selektive Informationen oder Dienste bereitstellen.

Struktur von Location Based Services



Nutzen von LBS-Anwendungen

Kundensicht

- Bequemlichkeit, Komfort
- Zeit- und Kostenersparnis
- Fähigkeit Personen oder Gegenstände zu verfolgen (tracken)
- schnellere Hilfe in Notfällen

Anbietersicht

- vereinfacht viele bestehende Anwendungen
- Angebot von personalisierten und ortsabhängigen Diensten
- ermöglicht neue Differenzierungsmerkmale

Datenschutzprobleme

Entgelt nur für erb. Dienste
Integrität der Nachrichten
Anonymität
Unbeobachtbarkeit
Unverkettbarkeit
Ortung mit Einwilligung
Bewegungsprofile
Interessenprofile

Nutzer

Mehrseitige Sicherheit

LBS-Anbieter

Zurechenbarkeit
Erreichbarkeit von Nutzern
Autorisierte Dienstnutzung

Netzbetreiber

Entgelt für erb. Dienste
Integrität der Nachrichten
Verfügbare Dienste

Bedrohungen

- Permanente und unbemerkte Observation möglich
  - Verletzung der Privatsphäre
  - Unternehmensspionage (Wer fliegt nach Shanghai?)
  - Militärische oder politische Spionage (Wo befindet sich der Bundeskanzler?)

- Ungewollte positionsbasierte Werbemaßnahmen

- Gefahr von gezielten Entführungen oder Anschlägen

Rechtliche Anforderungen, national

- National
  - Rechtsgrundlagen: Teledienstedatenschutzgesetz (TDDSG), Bundesdatenschutzgesetz (BDSG)
  - Erhebung von personenbezogenen Nutzungsdaten nur erlaubt, wenn diese zur Diensterbringung notwendig sind, beispielsweise zu Abrechnungszwecken (§6 TDDSG)
  - Nutzer muss vor Dienstbeginn über die Speicherung, Verwendung, Weitergabe und Speicherdauer personenbezogener Daten informiert werden (§4 TDDSG)
  - Standortdaten dürfen nur erhoben werden, sofern eine Einwilligung des Nutzers vorliegt (unabdingbare Voraussetzung)
  - Einwilligung kann elektronisch erfolgen, zurzeit besteht hier eine rechtliche „Grau-Zone“

Rechtliche Anforderungen, international (1)

- Vereinigte Staaten von Amerika

  - Phase I (Ende 1. April 1998):

    - Angabe der Telefonnummer jedes Notrufenden
    - Lieferung der Position, entweder Zell-Identifikationsnummer oder die Kennung der Base Station über die der Anruf erfolgte

Rechtliche Anforderungen, international (2)

- Vereinigte Staaten von Amerika

  - Phase II (noch nicht abgeschlossen):
    - Positionsangaben müssen in geographischen Längen- und Breitengraden ausgeliefert werden
    - Provider mit *netzseitiger* Positionsbestimmung (Zell-Id)
      - wenigstens 50% Gebiets- oder Bevölkerungsabdeckung bis 1. Oktober 2001
      - 100% Gebiets- oder Bevölkerungsabdeckung bis 1. Oktober 2002
      - 100 Meter Genauigkeit für 67% aller Notrufe und 300 Meter für 95% der Notrufe
      - Positionsschätzung für die restlichen 5 Prozent

Rechtliche Anforderungen, international (3)

- Vereinigte Staaten von Amerika
  - Phase II, Fortsetzung:
    - Provider mit *terminalbasierter* Positionsbestimmung (E-OTD)
      - Start des Geräteverkaufs bis spätestens 1. Oktober 2001
      - bis 31. Dezember 2001 müssen 25% der verkauften Neugeräte terminalbasierte Ortung unterstützen
      - 50% aller Neuverkäufe bis 30. Juni 2002
      - 100% aller digitalen Geräte bis 31. Dezember 2002
      - bis Dezember 2005 müssen 95% aller Mobilfunkteilnehmer ein Endgerät mit terminalbasierter Positionsbestimmung besitzen
      - 50 Meter Genauigkeit für 67% der Anrufe und 150 Meter für 95% der Notrufe
      - Positionsschätzung für die restlichen 5 Prozent

Rechtliche Anforderungen, international (4)

- Europa:
  - CGALIES (Coordination Group on Access to Location Information by Emergency Services)
  - arbeitet einen Plan aus, um die Bestimmung der Endgeräteposition in Notfällen europaweit zu standardisieren
  - Ziele der Work Group:
    - Definition von Voraussetzungen für Netzwerke, Datenbanken und PSAP (Public Service Answering Points)
    - Festlegung von Mindeststandards zu Methoden der Positionsbestimmung und Genauigkeit
    - Finanzierungs- und Kostenanalyse

Rechtliche Anforderungen, international (5)

- Europa
  - Probleme:
    - EU-Richtlinien verbieten die Ortung von Personen ohne ihre direkte Einwilligung → neue Richtlinie in Arbeit, die Ausnahme in Notfällen ermöglicht
    - bisher geringe Akzeptanz der 112-Nummer in Europa
  - angestrebte Genauigkeitsgrade: gewünscht / (gefordert)

	Indoor	**Urban**	**Suburban**	**Rural**	**Highway Crossroad**
Notrufende kann not-wendige Informationen selbst liefern	10 - 50 m	10 - 50 m (25 - 150 m)	30 - 100 m (50 - 500 m)	30 - 100 m (100 - 500 m)	20 - 100 m (100 - 500 m)
Notrufende ist nicht fähig, selbst Informationen zu liefern	10 - 50 m	10 - 50 m (25 - 150 m)	10 - 100 m (10 - 500 m)	10 - 100 m (10 - 500 m)	10 - 100 m (10 - 500 m)

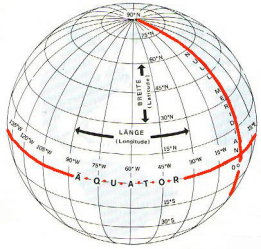
Positionsbestimmungsverfahren

- Wo wird die Position bestimmt?
  - Endgerät:
    - terminalbasierte Positionsbestimmung oder **Positioning**
    - Dienstnutzer empfängt Signale aus einem Netzwerk oder von installierten Sendern (Baken oder engl. Beacons) und berechnet auf Basis dieser seine Position selbst
  - Netz:
    - netzbasierte Positionsbestimmung oder **Tracking**
    - Dienstnutzer besitzt eine Kennung, die
      - von seinem Endgerät ausgestrahlt wird und die
      - vom Mobilfunk- oder einem Sensornetzwerk verfolgt wird

Handy mit IMSI

Badge mit Id

Repräsentationsformen von Positionsinformationen



- Koordinatensysteme
  - Absolute Positionsinformationen
    - GPS (Global Positioning System), Galileo
    - Postadresse
  - Relative Positionsangaben
    - Positionsangabe innerhalb eines WLAN-Systems

⇨ Transformation zwischen den Formaten möglich

- Symbolische Positionsangaben
  - Hierarchische symbolische Positionsangaben
    bspw. `/Deutschland/Bayern/Regensburg/Uni Reg/WiWi`
    ⇨ Umrechnung in physische Koordinaten möglich
  - Symbolische Positionsangaben mit logischen Aufenthaltsgebieten
    Beispiel: `/Post` oder `/Universität` (Bildung von Gruppen)
    ⇨ keine Transformation in Koordinatensysteme möglich

Positionsbestimmungsverfahren

- Wie wird die Position bestimmt?
  - Benutzereingabe
  - Aussenden von Positionsangaben
    - Positionssender
    - Cell-Id
  - Laufzeitmessung
    - Satellitengestützt
    - Uplink Time of Arrival (UL-TOA)
    - Enhanced Observed Time Difference (E-OTD)
  - Messung der Signalstärke
    - Location Fingerprint
  - Umgebungsanalyse

Benutzereingabe

- Eingabeformen:
  - Postleitzahlen, Ortsnamen und Straßennahmen
  - Manuelle Auswahl des aktuellen Standortes aus einer digitalen Karte
- Vorteile:
  - Benutzer kann auf die Genauigkeit Einfluss nehmen
  - Unabhängigkeit vom Endgerät
- Nachteile:
  - Benutzer muss seinen Aufenthaltsort kennen
  - Keine automatische Positionsbestimmung

Positionssender

- Funktion:
  - mobiles Endgerät empfängt von einem Positions-sender aktuelle Positionsdaten
  - potentielle Technologien für die Positionssender:
    - IrDA
    - Bluetooth
    - GSM-Netz (umgekehrtes Zell-Id-Verfahren)

Infrarot-Beacon
Entfernung: 2-25m

- Vorteile:
  - terminalbasierte Positionsbestimmung
  - Genauigkeit zwischen 1-25 Metern (Innenraum)
  - Sender könnten auch weitere Daten versenden

Infrarot-Beacon
großer Abstrahlwinkel

- Nachteile:
  - aufwändige Sendemontage
  - Endgeräteausstattung muss vorhanden sein

Zell-Identifikationsnummer (Cell-ID)

- **Bluetags** ist ein In- und Outdoor fähiges System zur Lokalisierung von Personen

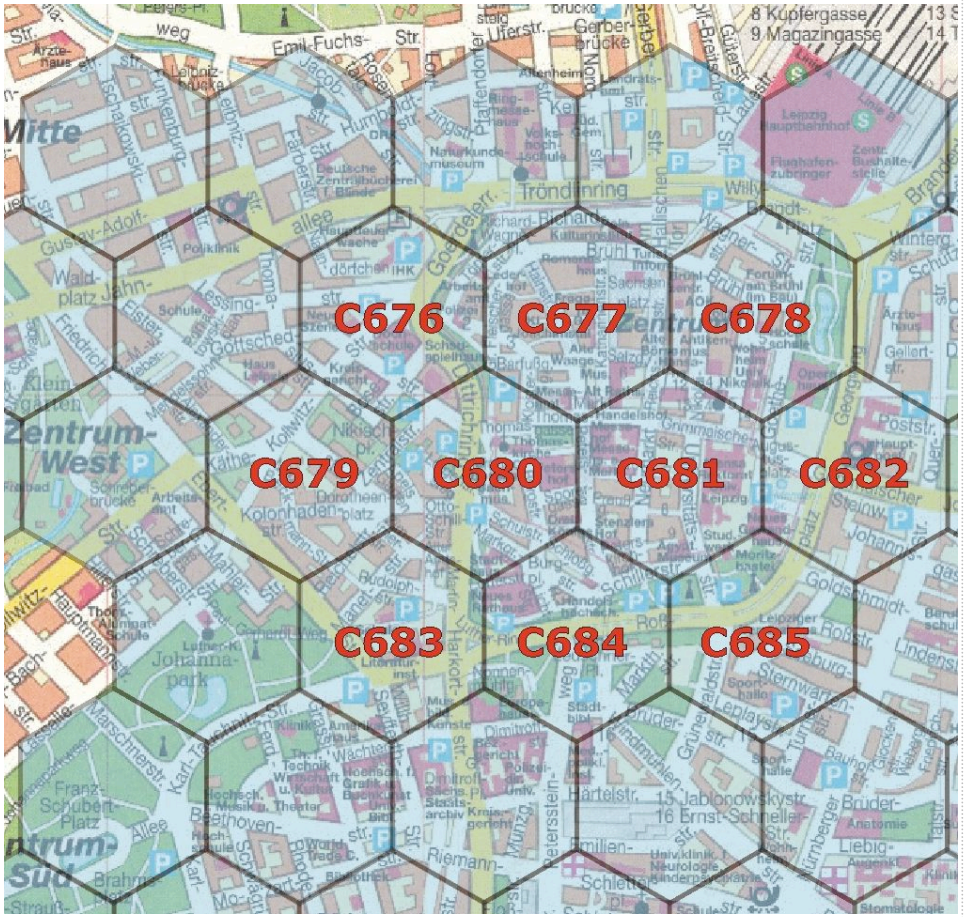
- Funktion:
  - Endgeräte werden permanent durch in Reichweite befindliche Access-Points lokalisiert (Genauigkeit 10-50 Meter)
  - ermittelte Positionsdaten werden über WLAN-Anbindung der AP an einen zentralen Server versendet

[www.bluetags.com]

- Anwendung:
  - dient zur Ortung von Kindern in Vergnügungsparks die ihre Eltern verloren haben (bspw. Tivoli Gardens)

Zell-Identifikationsnummer (Cell-ID)

- Funktion:
  - aktuelle Identifikationsnummer der Zelle, in der sich das Endgerät aufhält wird in einer Datenbank netzseitig gespeichert
- Vorteile:
  - sehr schnelle Lokalisierung
  - unabhängig vom Endgerät
- Nachteile:
  - Genauigkeit schwankt zwischen 300 Metern und 30 Kilometern
  - Positionsbestimmung erfolgt netzseitig



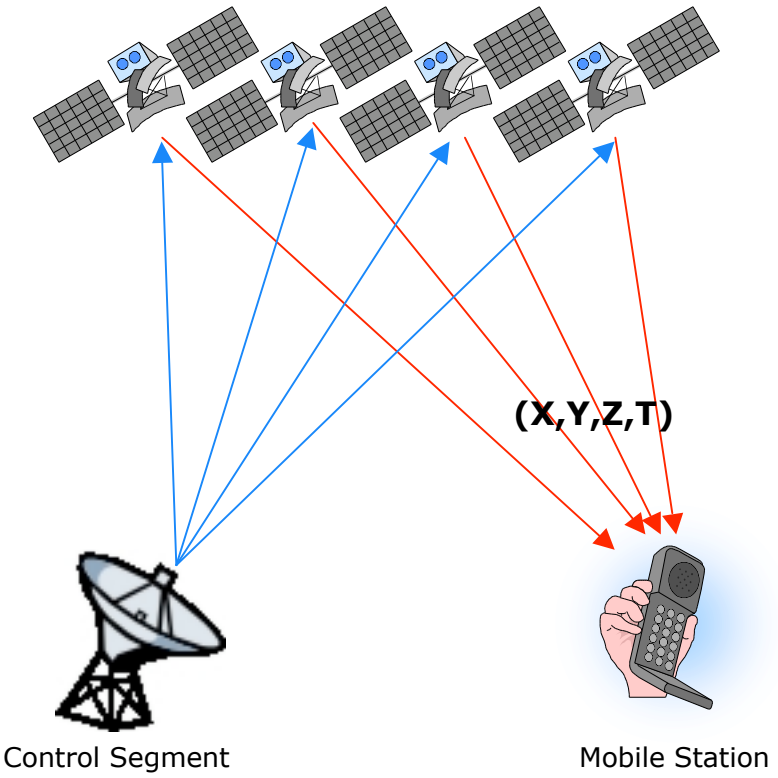
Satellitengestützte Ortung (1)

- Verfügbare Systeme:
  - NAVSTAR (GPS) – Vereinigte Staaten von Amerika
  - GLONASS – Russland
  - (Galileo) – Europa

- Aufbau und Funktionsweise von GPS:
  - 24 Low Earth Orbit (LEO) Satelliten
  - Service Level:
    - Standard Positioning Service (SPS)
      Präzision: 100m horizontal, 156m vertikal
    - Precise Positioning Service (PPS)
      Präzision: 22m horizontal, 27.7m vertikal
  - Selective Availability

Satellitengestützte Ortung (2)

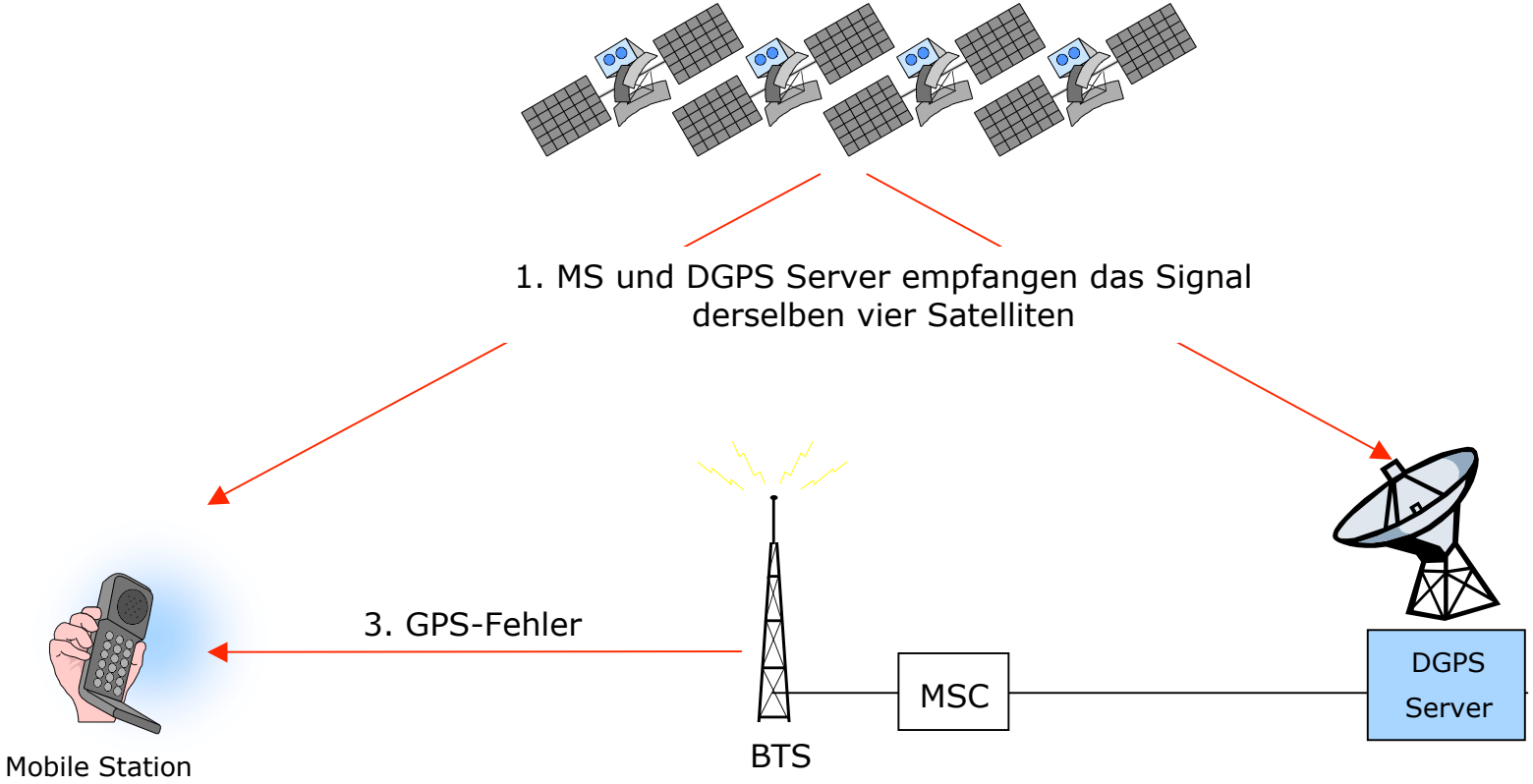
- Aufbau und Funktionsweise von GPS:
  - 4 Satelliten zur Positionsbestimmung notwendig
  - Satelliten übermitteln
    1. Almanac: enthält die groben Positionen der Satelliten
    2. Ephemeris: korrigierte Positionsdaten eines Satelliten (Gültigkeit: 4-6 Stunden)
    3. Uhrzeit
  - Positionsbestimmung durch Messung der Signallaufzeit



Satellitendistanz = Ausbreitungsgeschwindigkeit * Übermittlungszeit

Satellitengestützte Ortung (3)

- Differential GPS (DGPS):

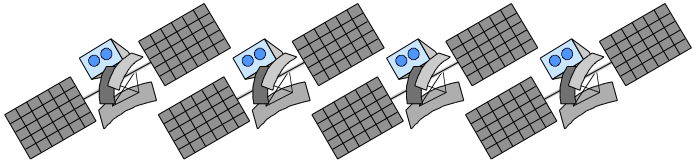


2. DGPS Server kennt seine genaue Position und berechnet für jeden sichtbaren Satelliten einen aktuellen GPS-Fehler

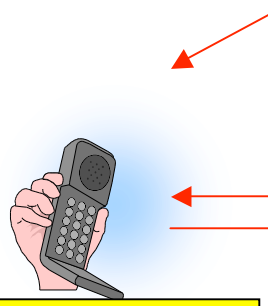
4. führt Messung durch und korrigiert diese mithilfe des vom DGPS-Server übermittelten GPS-Fehlers

Satellitengestützte Ortung (4)

- Assisted GPS:

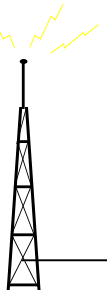


1. MS und A-GPS Server empfangen das Signal derselben vier Satelliten



3. Hilfsinformationen

5. Übermittlung der Messwerte



BTS

MSC

A-GPS Server

MS mit vereinfachtem GPS-Empfänger

4. führt genaue Messung durch

2. berechnet Hilfsinformationen zur schnellen Lokalisierung (doppler shift, Pseudo-Random-Noise phase)

6. berechnet genauen Ort

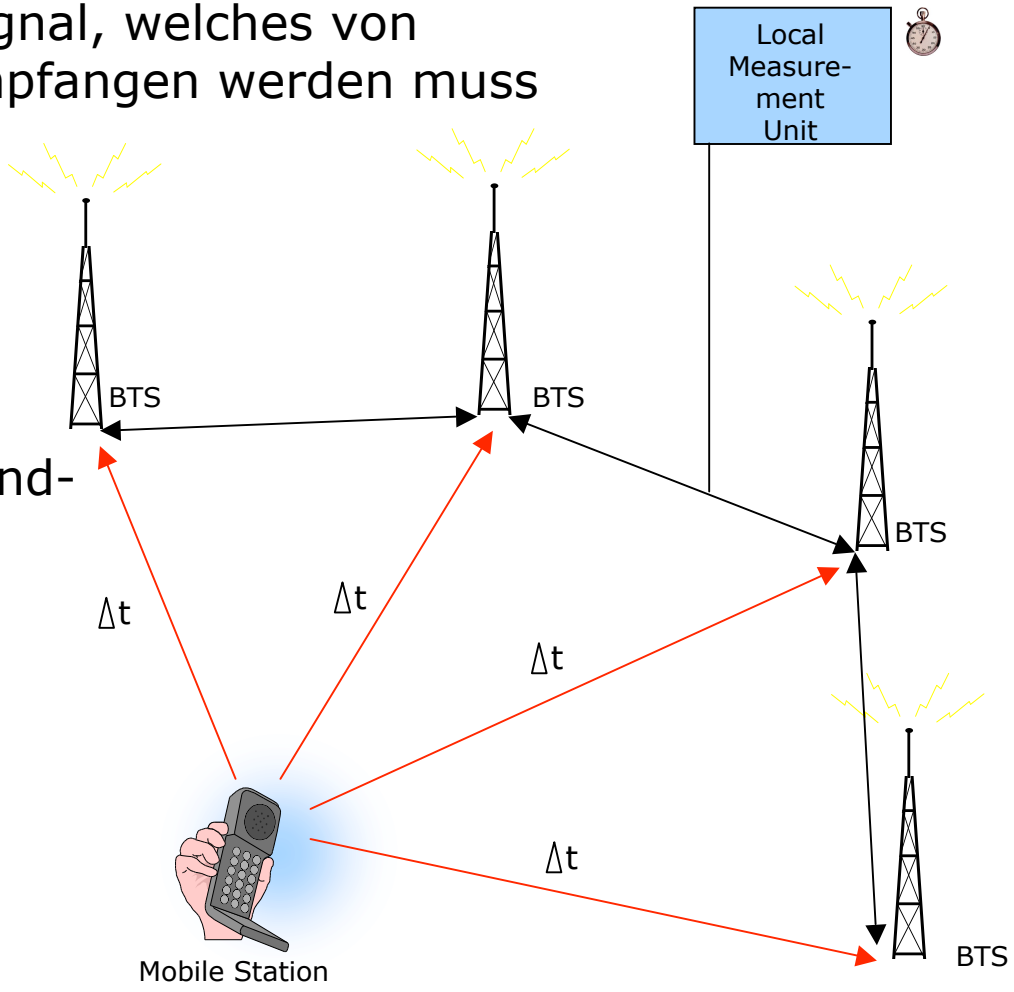
Satellitengestützte Ortung (5)

- Vorteile:
  - Positionsbestimmung sehr genau
    - normales GPS 10 bis 100 Meter
    - DGPS zwischen 1-5 Metern
  - Hohe Verfügbarkeit
  - GPS-Endgeräte relativ günstig
  - datenschutzfreundliche Positionsbe-stimmung

- Nachteile:
  - nur außerhalb von Gebäuden anwendbar
  - in stark bebauten Gebieten verschlechtern hohe Gebäude extrem die Dienstqualität
  - Lange Initialisierungsphasen (laden des Almanac)
    → u.U. ungeeignet für Notrufsituationen
  - Selective Availability

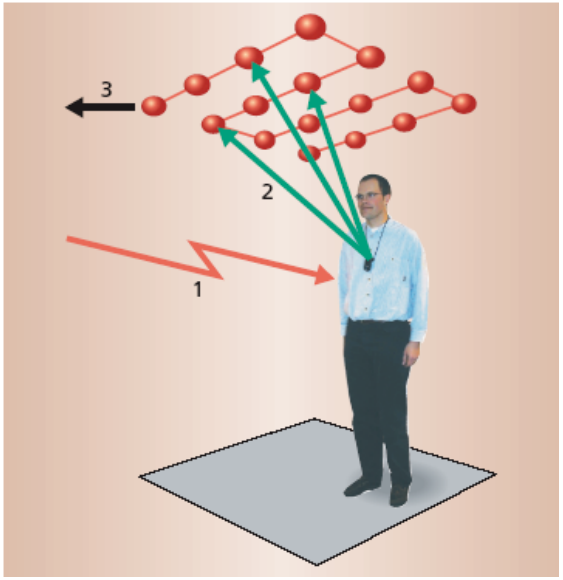
Uplink Time of Arrival (UL-TOA)(1)

- Funktion:
  - die MS versendet ein Signal, welches von mindestens vier BTS empfangen werden muss
  - BTS bestimmen Signal-laufzeit und berechnen Position der MS
- Vorteile:
  - keine Änderungen am End-gerät
  - geringe Antwortzeiten
- Nachteile:
  - netzseitige Positionsbe-stimmung
  - hohe Kosten für die Infrastruktur



Uplink Time of Arrival (UL-TOA)(2)

- Das **Bat-System** ist eine Indoor-Variante zur Positionsbestimmung von AT&T
  - Genauigkeit: < 1 Meter
  - zentraler Controller notwendig



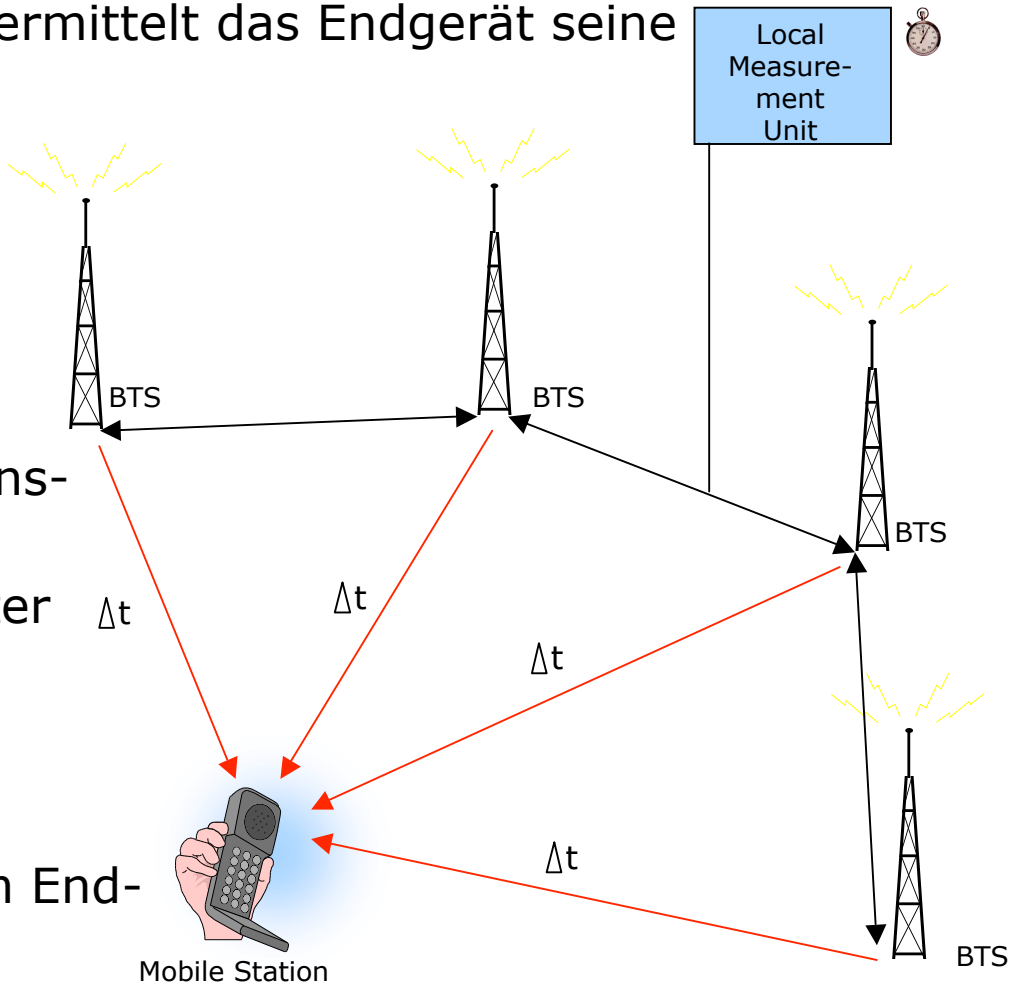
[IEEE Computer August 2001, S. 2-9]

1. Ständige Verbindung zu einem lokalen Funknetzwerk
2. Bat sendet periodisch Funksignal aus, welches von Beacons empfangen wird
3. Ein zentraler Server berechnet aus der Signallaufzeit die Distanz

- Vorteil:
  - hohe Genauigkeit
- Nachteile:
  - hoher Installationsaufwand der Beacons
  - netzseitige Positionsbestimmung
  - schlechte Skalierbarkeit

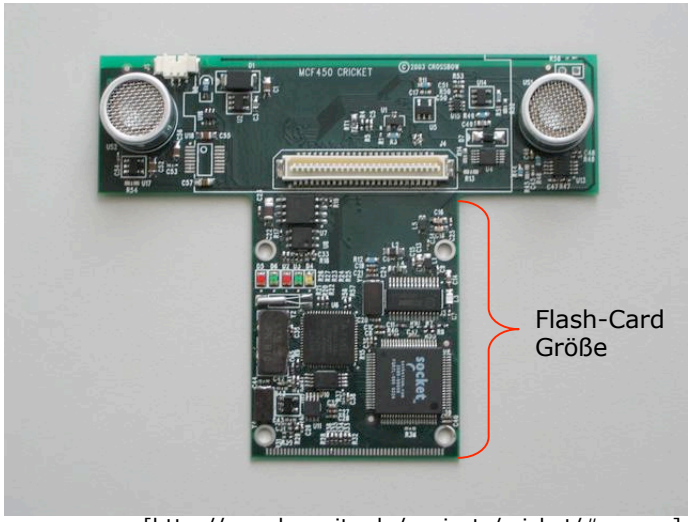
Enhanced Observed Time Difference (E-OTD)(1)

- Funktion:
  - durch Laufzeitmessung ermittelt das Endgerät seine aktuelle Position
  - BTS versenden in regelmäßigen Abständen Signalfolgen (Burst)
- Vorteile:
  - endgeräteseitige Positionsbestimmung
  - Genauigkeit 50-100 Meter
  - Schnelligkeit
- Nachteil:
  - Softwareupdate auf dem Endgerät notwendig

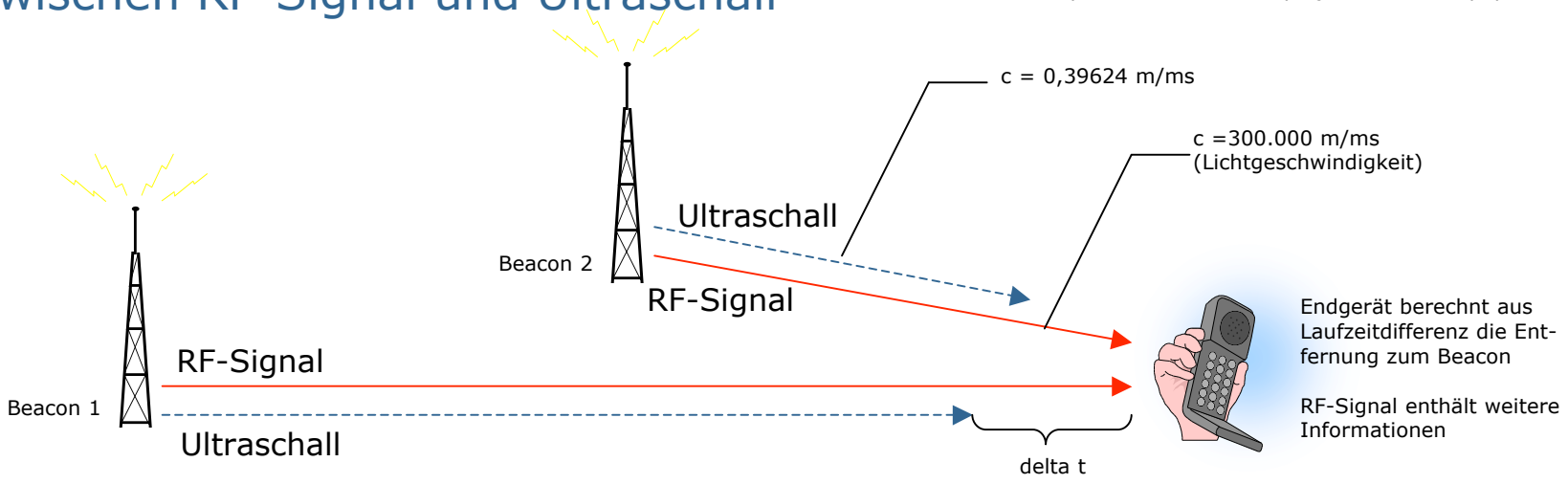


Enhanced Observed Time Difference (E-OTD)(2)

- Cricket ist ein Indoor-Positionsbestimmungssystem und wurde im Project „Oxygen" am MIT entwickelt
- im Raum angebrachte Beacons senden gleichzeitig ein RF- und Utraschall-Signal aus
- Distanz zwischen Beacon und Endgerät ergibt sich aus der Laufzeitdifferenz zwischen RF-Signal und Ultraschall



[http://nms.lcs.mit.edu/projects/cricket/#papers]



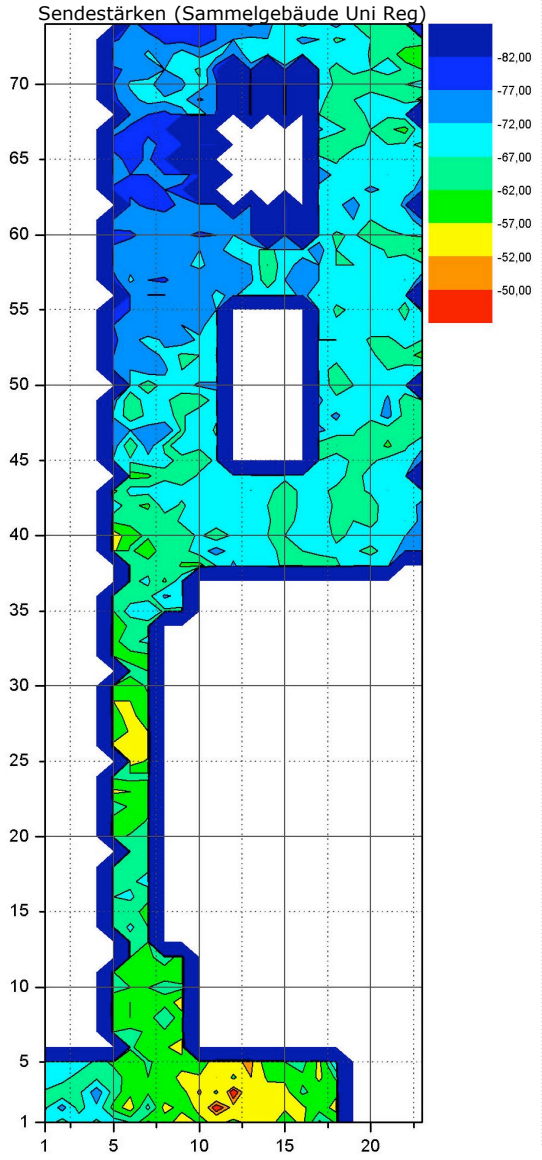
Signalstärke - Location Fingerprint

- Funktionsweise:
  - Endgerät misst von allen sichtbaren Sende-masten die Empfangsstärken

    ⇩

    Location Fingerprint

  - Position kann durch Nachschlagen in einer Datenbank bestimmt werden
- Vorteile:
  - Nutzung bestehender Infrastrukturen
  - Verwendung innerhalb von Gebäuden
  - Genauigkeit zwischen 3 und 15 Metern
- Nachteile:
  - hohe Anforderung an Endgeräteausstattung
  - Empfindlichkeit gegen Störungen sehr hoch



Umgebungsanalyse (1)

- Funktionsweise:
  1. Im städtischen Umfeld werden alle Gebäude dreidimensional erfasst
  2. Dienstnutzer fotografiert eine Szene in seiner Umgebung und schickt dieses Bild zur Analyse an einen Server
  3. Zentraler Server ermittelt Position

- Vorteile:
  - Genauigkeit soll bis zu 1 Meter betragen
  - Kameras bereits in vielen Mobiltelefonen integriert

- Nachteile:
  - hoher Ersterfassungsaufwand der Umgebung
  - nicht überall einsetzbar (bspw. militärische Anlagen)
  - sehr empfindlich gegenüber Änderungen in der Umwelt
  - nicht zur permanenten Positionsbestimmung geeignet

- Prototyp wurde an der Cambridge University entwickelt

Umgebungsanalyse (2)

Taking a picture with a camera phone to find out where you are

The original photo is sent to a server

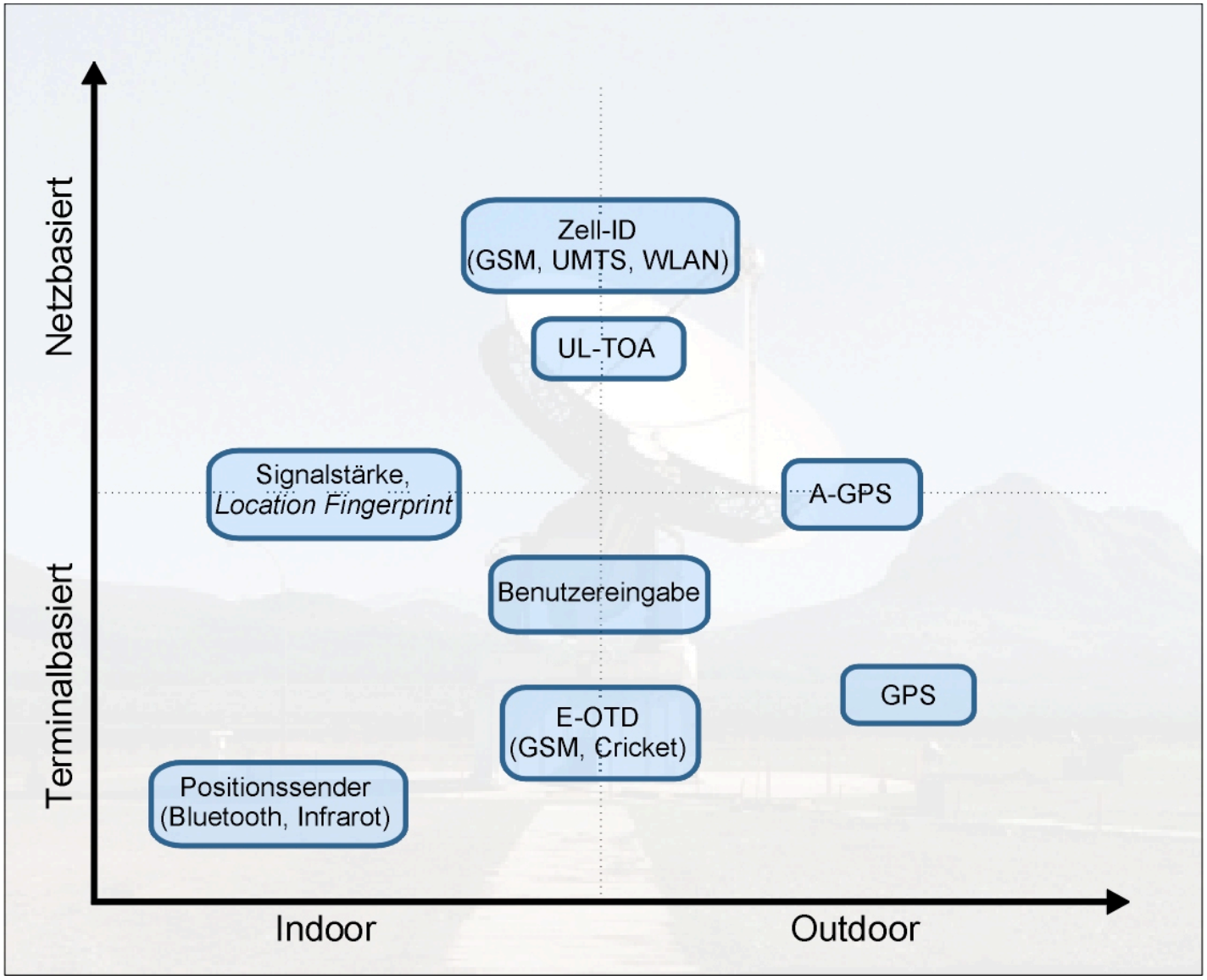
Software on the server identifies horizontal and vertical edges

Using the edges, the image is distorted so that it looks as though the photo was taken face-on

Software locates key points in the image, such as corners, which are then matched to images in the database

SOURCE: DUNCAN ROBERTSON, CAMBRIDGE UNIVERSITY

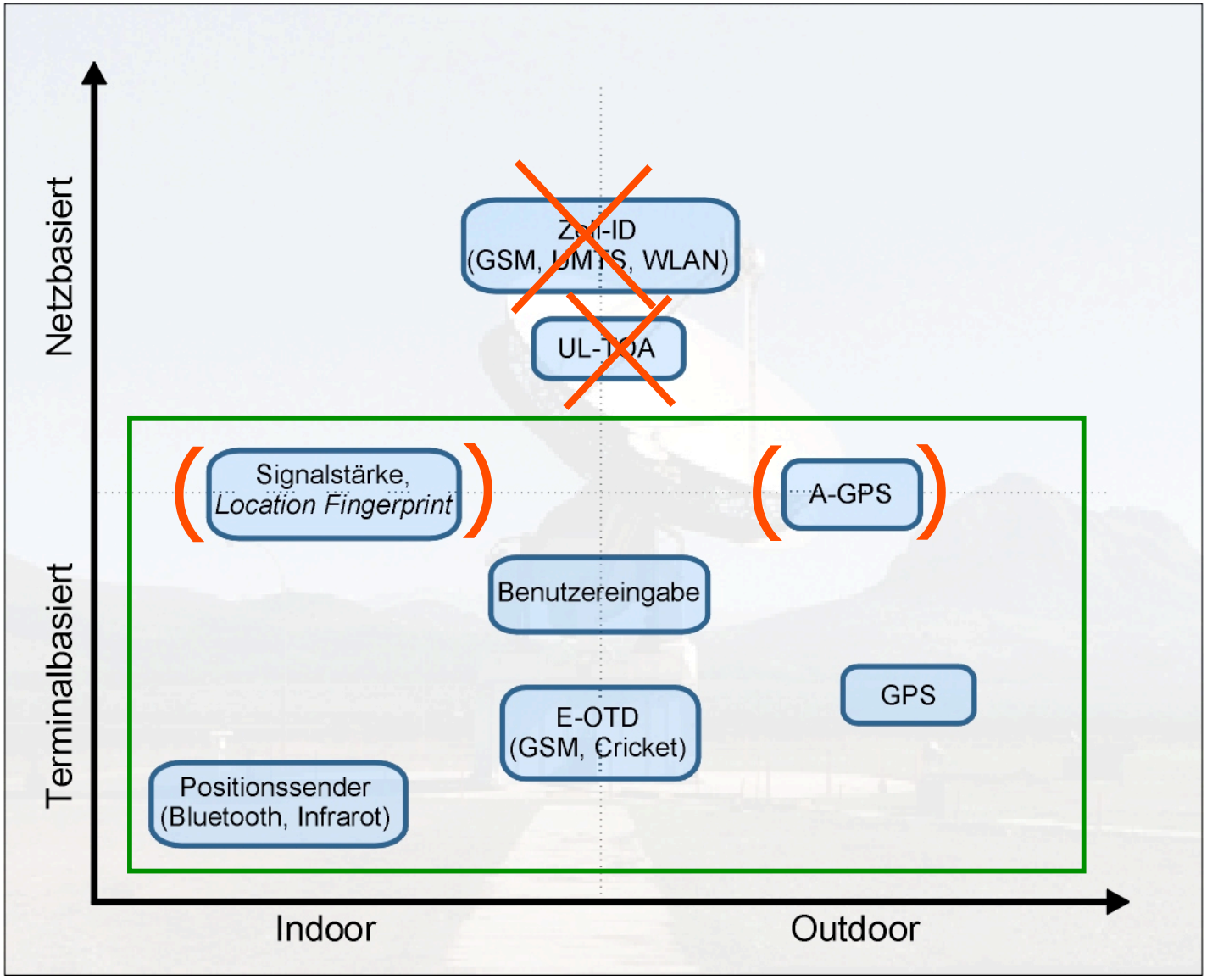
Positionsbestimmungsverfahren



Positionsbestimmungsverfahren und Datenschutz

- Netzbasierte Positionsbestimmung
  - Positionsbestimmung ausschließlich durch Netzbetreiber
  - Nutzer hat keine Kontrolle über die Verwendung der erhobenen Daten, weshalb aus Datenschutzsicht diese Verfahren zu vermeiden sind
- Terminalbasierte Positionsbestimmung
  - Ermittlung des eigenen Standortes ausschließlich im mobilen Endgerät
  - gibt dem Dienstnutzer volle Kontrolle über die ermittelten Koordinaten, ohne dass einem Dritten vertraut werden muss

Positionsbestimmungsverfahren



Standards und Protokolle

- Ziele: Location Based Services müssen
  - unterschiedliche Positionsbestimmungstechnologien
  - mehrere Transportprotokolle und
  - verschiedenste Infrastrukturen

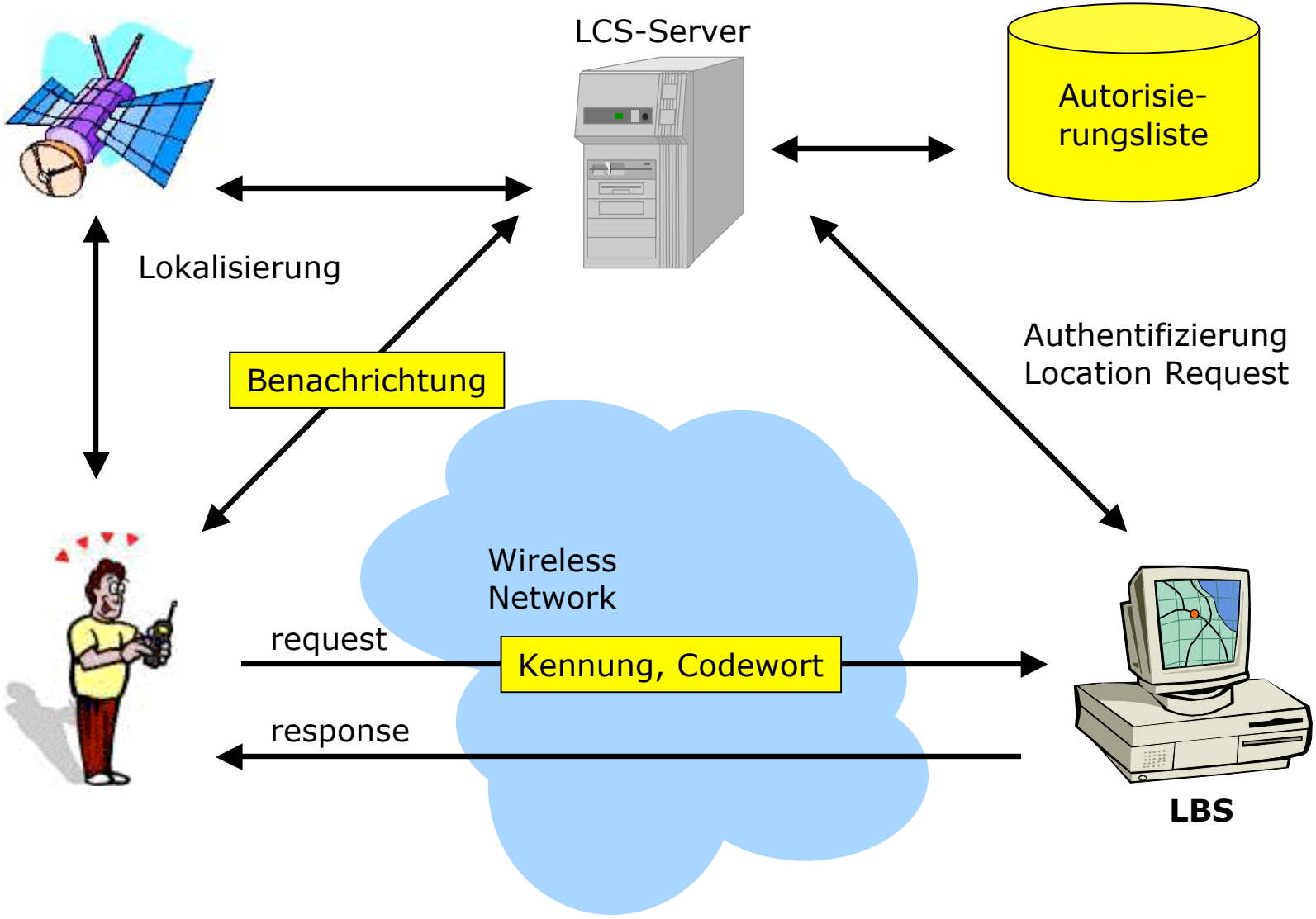
  unterstützen.
- Es sollten einheitliche und global verwendete Standards für Location Based Services entwickelt werden.

- Standards und Protokolle
  - 3rd Generation Partnership Project (3GPP)
    - Location Service (LCS) Standard
  - Location Interoperability Forum (LIF)
    - Mobile Location Protokoll (MLP)
  - Internet Engineering Task Force (IETF)
    - Geographic Location Privacy (Geopriv)

Standards und Protokolle

- Location Service (LCS) Standard
  - 3rd Generation Partnership Project (3GPP)
  - Verabschiedung von der ETSI
  - Ziel
    - Integration von LBS in GSM- und UMTS-Netzen zu standardisieren
  - Leistungsfähigkeit
    - Abfrage und Übermittlung von Positionsinformationen
    - Autorisierung der Datenweitergabe durch Nutzer
  - Entwicklungsstand
    - für sehr konkrete Zielsysteme geschaffen
    - daher direkt umsetz- und nutzbar
    - jedoch begrenzter Einatzbereich und Verallgemeinerungsgrad

Architektur vom LCS



Standards und Protokolle

- Mobile Location Protokoll (MLP)
  - Standardisierung vom Location Interoperability Forum (LIF)
  - Ziel:
    - Kommunikation von LBS-Anwendungen mit so genannten Location Servern ermöglichen
  - Leistungsfähigkeit
    - Abfrage von Positionsinformationen
    - unabhängig von der Positionsbestimmungsmethode
    - unabhängig vom zugrunde liegenden Datenübertragungsprotokoll
  - Definiert eine Schnittstelle, die den Austausch von Standortinformationen ermöglicht
    - Verwendung von XML

Standards und Protokolle

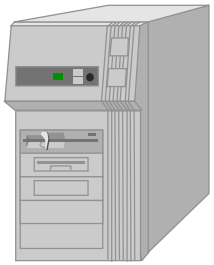
- MLP-Protokoll-Typen:
  - Standard Location Immediate Service
  - Emergency Location Immediate Service
  - Standard Location Reporting Service
  - Emergency Location Report
  - Triggered Location Reporting Service

```
<?xml version="1.0" ?>
<!DOCTYPE slia SYSTEM "MLP_SLIA_200.DTD">
<slia ver="2.0.0" res_type= "PERSISTENT">
  <pos>
    <msid>461011334411</msid>
    <pd>
      <time utc_off="+0200">20000623134453</time>
      <shape>
        <circle>
          <point>
            <ll_point>
              <lat>301628.312</lat>
              <long>451533.431</long>
            </ll_point>
          </point>
          <rad>240</rad>
        </circle>
      </shape>
    </pd>
  </pos>
```

[LIF TS 101 v2.0.0, S. 27]

MLP

Location-Server



Location Request

über standardisierte schnittstelle (Internet / HTTP / HTTPS / ...)

Lokalisierung

request / response

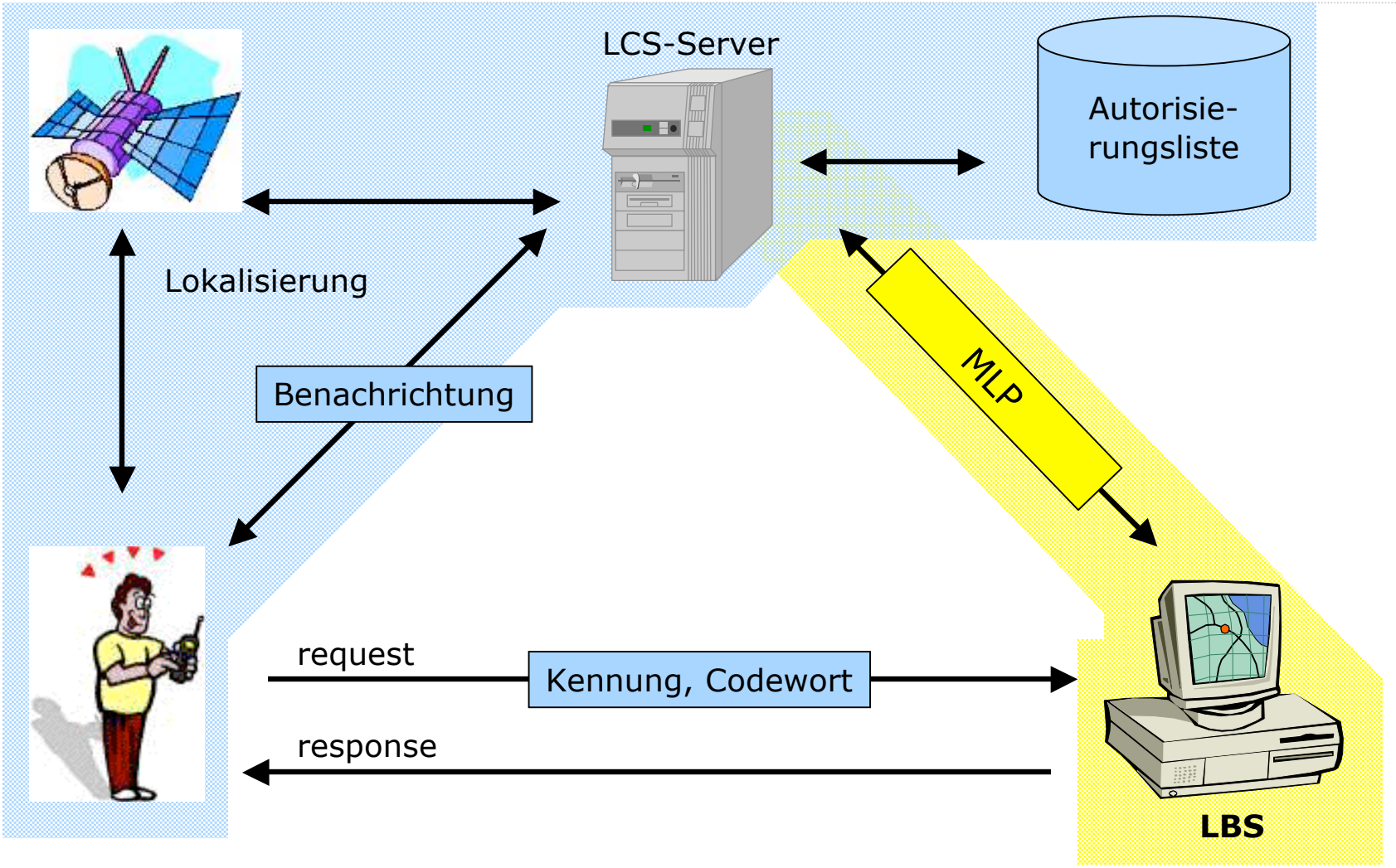
Wireless Network

request

response

LBS

Vergleich LCS — MLP

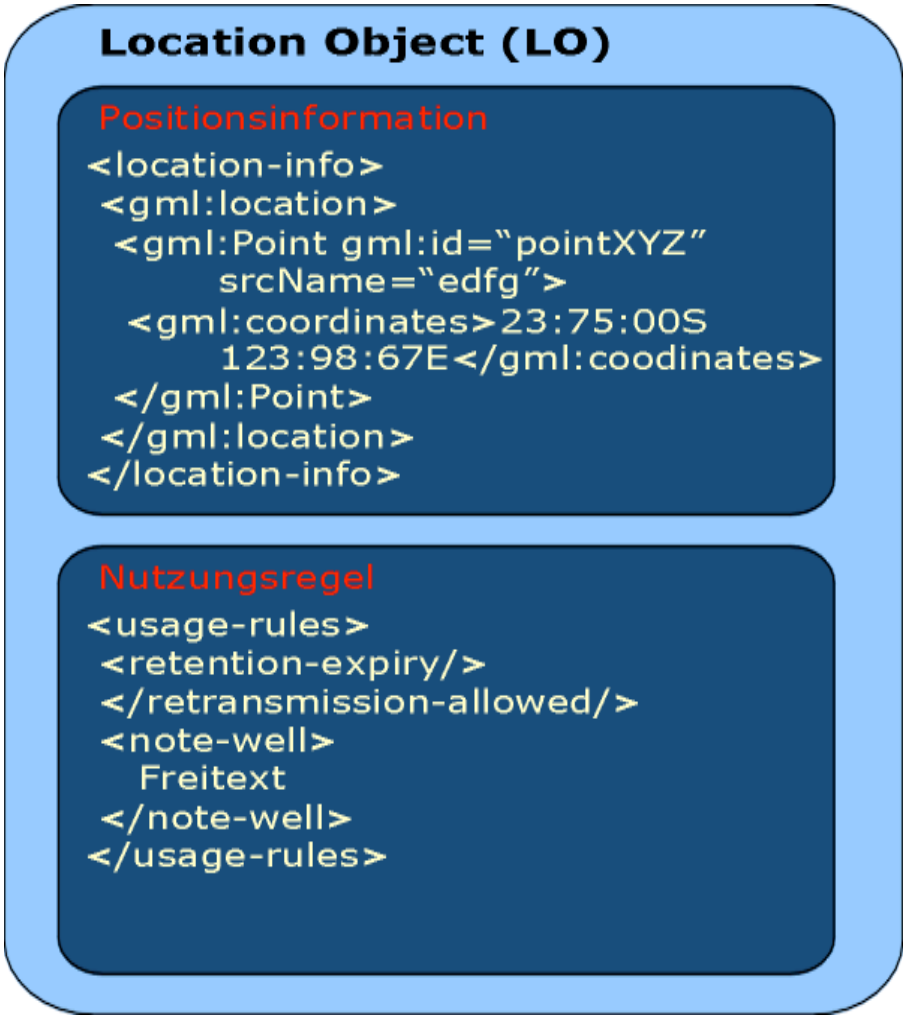


Standards und Protokolle

- Geographic Location Privacy (Geopriv)
  - Entwicklung der Internet Engineering Task Force (IETF)
  - Ziel
    - Definition eines Containers (Location Object, LO) für die vertrauliche Speicherung von Ortsdaten
    - keine konkrete Definition des Datenformats
  - Leistungsfähigkeit
    - schafft es eine Architektur zur sicheren Übertragung von Dokumenten
    - definiert einen „Briefumschlag“, in dem jedes XML-basierte Dokument transportiert werden kann
    - Verschlüsselung und Signaturen möglich

Standards und Protokolle

- Geographic Location Privacy (Geopriv)



Schlussbemerkungen

Treiber	Hemmnisse
	• keine verlässliche Genauigkeit einiger Verfahren
• Schaffung höherer Sicherheit (Notfall)	• Sicherheits- und Datenschutzbedenken
	• unzureichende Standardisierung
• Positionsinformation als Erfolgsfaktor für neue mobile Anwendungen	• Mangel an sinnvollen Anwendungen

Terminalbasierte Verfahren sind datenschutzfreundlicher.
Lokalisierung durch das Netz ist nicht verhinderbar.