Geolocalisation in Cellular Telephone Networks

Bruce Denby
Université Pierre et Marie Curie – Paris VI
Laboratoire d’Electronique
Ecole Supérieure de Physique et Chimie Industrielles de la Ville de Paris
10 rue Vauquelin
Paris, France
bruce.denby@gmail.com
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
What is Cellphone Localisation?

- Cellphones can be used anywhere
  - Indoors or outdoors
  - In a car, bus, train, or boat
  - In a crowd, or all alone
  - On top of a building, or in a parking garage
- Localisation technology inserts new fields into the Call Detail Record of a cellphone communication, allowing to estimate the calling party’s location
- What precision is possible?
  - Outdoor: several tens of meters
  - Indoor: it’s still a research area, but a few meters is a reasonable guess

“Where’s the party?”
Why Localise Cellphones?
Emergency Services

• Fixed line calls to 911 can be localized to a street address
• The E911 mandate launched in the US in 1999 requires cellular operators to localize 911 calls from cellphones:
  – Network based: 67% of calls at \( \leq 100\text{m} \)
    95% of calls at \( \leq 300\text{m} \)
  – Mobile based: 67% of calls at \( \leq 50\text{m} \)
    95% of calls at \( \leq 150\text{m} \)
• E112 was launched in 2003 to do the same thing in Europe
Why Localise Cellphones?
Location Based Services

• “Push” advertising
  – Big sale at Crate & Barrel down the street
  – Grand opening of a new Baskin-Robbins nearby…

• Navigation
  – Nearest bank, florist, restaurant, etc.
  – Directions to an address
  – Next bus…

• Social/family
  – Friends map
  – Dating services
  – Child monitoring…

Example:
Why Localise Cellphones? Health Care and Family Security

• Tracking of elderly persons or persons with medical conditions
  – “Place logging”: market, doctor, library, friend’s house, etc.
  – Indoor tracking: bedroom, bathroom, kitchen, living room…
  – Moving or still?
  – Prolonged period of
  – inactivity?

• Monitoring of family members
Why Localise Cellphones?
Customer Behaviour Monitoring

• Location based billing:
  – Fixed rates at home and work
  – Special rates in other zones…

• Analyse customers’ movement habits, correlate with other factors

• Detect possible subscription fraud from inhabitual patterns of movement
Why Localise Cellphones?
Law Enforcement and Forensics

- Subscription fraud (illegally sold services) annual cost to telecom industry $35 billion
- Tracking persons or vehicles in cases of kidnapping or other serious crimes
- Detect unauthorized usage of cellphones (prison, restricted area…)
- Forensic analysis of call records to establish the whereabouts of a suspect at a particular time (*alibi* verification)
- Problem: what is the exact “coverage area” of a particular cell tower?
Why Localise Cellphones?
National and International Security

- Espionage and counterespionage
  - “Fake” BTS used to crack encryption security
- Person tracking in cases of suspected terrorist activity
- Recent Issue: The NSA has requested huge volumes of CDR’s of everyday citizens. What information is contained in these files?
  - The EU Data Retention Directive instated in March 2006 appears to be intended for similar purposes
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
How do Cellphones Work, Anyway?

MS - Mobile System (Cellphone)
BTS - Base Transceiver Station (Cell Tower)
BSC - Base Station Controller
OMC - Operations and Maintenance Center
BSS - Base Station Subsystem
MSC - Mobile System Switching Center
VLR - Visitor Location Register (Roaming)
HLR - Home Location Register (Authentication, Billing)
PSTN - Public Switched Telephone Network (Landline)
LMU - Location Measuring Unit (if Location Services implemented)
Call Detail Records

- The CDR is a billing mechanism originating in fixed line communications: who called whom and for how long?
- CDR’s initially came out of the exchange hardware on a serial port for printing.
- Today CDR’S are stored in databases, which are saved for 30-60 days depending on the operator
- The baseline record format of CDR’s is:
  - Calling and called numbers
  - Channel number
  - Date and timestamp
  - Elapsed time
  - Call failure class if any
  - Billing amount
Modern CDR Databases

- Cellphone CDR’s contain additional fields due to the complexity of cellular networks.
- In addition, cellular operators can insert new record types, some of which may be proprietary.
- A major telecom carrier generates hundreds of millions of CDR’s per day, corresponding to terabytes of data.
- These new, richer CDR databases can be analysed to extract information of different types, including localisation.
- The CDR files must be processed in real time to provide customers immediate access to billing information, and for law enforcement and security requests.
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
Cellphone Localisation Methods

- Cellphone systems were designed for communications
- Localisation is an add-on
- Solutions adopted for localisation
  - Should use existing infrastructure or involve minimal upgrades (e.g., Location Measuring Units, LMU)
  - Should if possible work with “legacy” phones
- Targeted performance: a few meters, indoor or outdoor
Can’t We Just Use GPS?

- GPS: network of 24 satellites for terrestrial navigation applications
- Standard GPS has a resolution of ~10m, less than 1m in differential mode (DGPS)
- Some cellphones already have built-in GPS receivers
- The trend is full GPS integration using small, light, low power GPS chips
- Main problems:
  - Large numbers of legacy phones do not have GPS chips
  - GPS satellite coverage is poorly adapted to localisation of cellphones carried by pedestrians... العنوان
Cellphone GPS Reception

- GPS requires at least 4 locked-in satellites to function correctly, with localisation precision increasing with number of satellites.
- “Urban canyon” environments very often do not offer enough visibility to lock in 4 satellites, especially in pedestrian scenarios.
- Lock-in times are also longer when satellite visibility is marginal or variable.
- GPS does not work at all in indoor!!
- Indoor and deep urban environments are of primordial interest for emergency services, person tracking, law enforcement, etc…
Radio Interface Techniques

- Exploit existing location-dependent network variables
  - Cell ID, Received Signal Strength (RSS), Timing Advance (TA)...
- Use information from the cellphone
  - Amplitude, frequency, timing, and directional information of electromagnetic signals emitted and received by the cellphone
Radio Interface Techniques
Cell ID

• The simplest method
  – Use the position of the current serving BTS (cell tower)
• This is already pretty good in dense urban environments
  – Where a picocell radius can be less than 100m
  – Though maximum GSM cell radius is 35 km…
• In general we would like to do better
Radio Interface Techniques
Cell ID+TA

• Timing Advance TA is a (GSM) network variable
  – It accounts for propagation time between the MS and the BTS

• Unfortunately:
  – The position resolution of TA is \( c \cdot T_{\text{bit}} = 500\text{m} \) (GSM)

• For CDMA (3G networks)
  – \( c \cdot T_{\text{chip}} = 35\text{m} \),
  – But *multipath* effects make it impossible to achieve this resolution in practice
Radio Interface Techniques
“Triangulation”

- Better resolution is possible by measuring the time delay at 3 BTS:
  - Observed Time Delay of Arrival (O-TDOA) and similar methods
- This requires synchronised BTS
- Can be accomplished with LMU’s but is costly
- Also, multipath effects compromise the possible resolution
Radio Interface Techniques
Angle of Arrival AOA

• The MS can also be pinpointed by detecting the angle of arrival of its signal at two BTS
• This requires directional antennas at the BTS and is thus costly
• The technique is also compromised by multipath effects
Multipath and Mask Effects

- In urban environments the received signal is a superposition of direct, reflected, and diffracted rays.
- In Non-Line of Sight (NLOS) situations the direct ray is masked.
- This degrades performance of timing and angle based solutions since each path has a different delay and angle.
- Multipath and mask effects are also important in indoor propagation channels.
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
Database Correlation Technique

- Many organisms now use radio fingerprinting for localisation.
- In order to always be ready for a handover, the GSM norm requires mobiles to send regular (~1Hz) Network Measurement Reports (NMR) to the BTS.
- These contain signal strengths of the serving cell and the 6 strongest neighbours.
- This is a “fingerprint” of the local radio environment.

<table>
<thead>
<tr>
<th>BTS</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMR</td>
<td>1</td>
<td>22</td>
<td>13</td>
<td>11</td>
<td>15</td>
<td>35</td>
<td>25</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td>9</td>
<td>15</td>
<td>24</td>
<td>67</td>
<td>35</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Database Correlation Technique
Example Measurement Report

- **timestamp**: 15:36:04.46
- **Latitude and Longitude**: N 48°49.9910 L 002°21.6970
- **Frame number**: 569702
- **Serving Cell signal strength**
- **Measurements are valid**
- **Neighbour cell number** (top 6 cells)
- **Received Signal Strength (RSS) of neighbour cells**
- **Cell ID code**
- **Cell frequency code**
Database Correlation Technique
Localising w/ Radio Fingerprints

• Generate a database of previously recorded fingerprints that have been position-labelled using GPS or some other standard geolocalisation technique

• To localise a mobile
  – Check NMR against database
    • With whichever ML technique (k-nn, SVM, …)

• The database correlation method
  – Automatically takes into account multipath and mask effects.
  – It uses the standard GSM norm and involves no changes to handsets or infrastructure: 😊
Database Correlation Technique
Fingerprinting Challenges I

• For good precision, a fine measurement grid is needed
  – Expensive and time-consuming to populate database
    → Semi-supervised techniques
  – Requires trace tools (see demo later)

• Received Signal Strength *predictions* can also be used
  – Less accurate
  – Require operator information, expertise, and software tools

• RSS measurements at a given position are quite variable
  – Follow a Rayleigh distribution
  – Seldom find exactly the same 7 cell towers – problem of imperfect matches
  – RSS varies
    • with meteorological conditions (dry/rain)
    • with the season (foliage effects)
Database Correlation Technique
Fingerprinting Challenges II

• Cell tower positions and labels may be unknown or time-dependent
  – The operator may not want to divulge his tower locations
  – There may be added or displaced towers – BTS, a new frequency plan, revised numbering scheme, etc.
    → Semi-supervised techniques

• Database management issues
  – Database is very large & very sparse
    • Thousands of BTS for a big city
    • Combinatorics of subsets of 7 (contents of an NMR)
  – Path loss assures ‘locality’
    • Only a subset of BTS is important at a given position

• Data volumes & Real time constraint
Database Correlation Technique Experiment

- 100 km of GSM *in-car* traces: Paris, France
  - Recorded with TEMS system
- Data labelled with ground coordinates
  - Recorded simultaneously with a GPS
- About 3 hours of talk over a 5 day period
- 6700 Network Measurement Reports
- 4000 used for training, 2700 for validation
  - 10-fold cross validation
Database Correlation Technique
Experiment – Trace Routes
Database Correlation Technique
Experiment – Analysis Techniques

• Problem

  – Use vectors of 7 non-zero values
    • RSS of the serving cell and 6 strongest neighbour cells
  – to predict the GPS coordinates of the mobile user

• Possible techniques

  – SVM (regression)
  – k-NN
  – HMM (take into account movement of mobile…)
  – Model RSS as a “Gaussian process” (max. likelihood)
  – your idea here …
Database Correlation Technique
Experiment – Preliminary Results

95% of sites to 60 meters or less
67% of sites to 10 meters or less
• Average results over 10 random splits
• No technique is always better
• A very good result but, on a sparse grid…?
Database Correlation Technique
Indoor Fingerprint Localisation

• **GSM** has good indoor penetration

• Absorption of radio signals from the surrounding BTS by structural elements is highly variable according to exact cellphone position (😊!!)

• Preliminary studies at our lab show room-level localisation (classification problem) efficiency near 100% using SVM or kNN.
Database Correlation Technique
WiFi Indoor Fingerprint Localisation

• Can also do indoor fingerprinting with WiFi
• Some cellphones can connect to WiFi…
• Are there enough access points visible in a home environment?
• More appropriate for workplace, airport…?
• The ICDM 2007 Data Mining Contest is on Indoor WiFi localisation via fingerprinting
  – http://www.cse.ust.hk/~qyang/ICDMDMC07/
  – Only 10% of the data is labelled
  – Results due 26 September 2007!
Database Correlation Technique
Hybrid Method: Assisted GPS

- A GPS-equipped cellphone showing less than 4 visible satellites relays the partial information to the network along with a radio fingerprint.
- The network is able to resolve the ambiguity in many cases and return the correct position information to the mobile.
- Assisted GPS is under test by some operators.
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
### Standard LCS CDR Entry

**LCS = Location Service**

**International Mobile Subscriber Identifier (IMSI)**

**Subscriber phone number**

**Latitude & Longitude**

**Localisation method used**

**Time stamp**

**Operator specific extensions**

#### 6.1.3.1 LCS Records for Mobile Originated Location Request (LCS-GMO-CDR)

If enabled, a LCS GMLC Mobile originated Charging Data Record (LCS-GMO-CDR) shall be produced for each mobile originated location request performed via the GMLC. The fields in the record are specified in table 6.1.3.1, which provides a brief description of each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Type</td>
<td>M</td>
<td>LCS GMLC Mobile Originated Record</td>
</tr>
<tr>
<td>Recording Entity</td>
<td>M</td>
<td>The E.164 address of this GMLC</td>
</tr>
<tr>
<td>LCS Client Type</td>
<td>C</td>
<td>The type of the LCS client that invoked the LR, if available</td>
</tr>
<tr>
<td>LCS Client Identity</td>
<td>C</td>
<td>Further identification of the LCS client, if available.</td>
</tr>
<tr>
<td>Served IMSI</td>
<td>M</td>
<td>The IMSI of the subscriber that requests the location.</td>
</tr>
<tr>
<td>Served MSISDN</td>
<td>Om</td>
<td>The primary MSISDN of the subscriber that requests the location.</td>
</tr>
<tr>
<td>Serving Entity</td>
<td>C</td>
<td>The E.164 address of the serving MSC (in case of CS-MO-LR) or SGSN (in case of PS-MO-LR)</td>
</tr>
<tr>
<td>Location Estimate</td>
<td>Om</td>
<td>The location estimate for the subscriber if contained in geographic position and the LR was successful.</td>
</tr>
<tr>
<td>Positioning Data</td>
<td>C</td>
<td>The positioning method used or attempted, if available.</td>
</tr>
<tr>
<td>User Error</td>
<td>C</td>
<td>The Location Service type of error if any failure happened</td>
</tr>
<tr>
<td>Provider Error</td>
<td>Om</td>
<td>The protocol related type of error if any failure happened</td>
</tr>
<tr>
<td>Record Time Stamp</td>
<td>Om</td>
<td>Time of generation of the CDR</td>
</tr>
<tr>
<td>Local Record Sequence Number</td>
<td>Om</td>
<td>Consecutive record number created by this node. The number is allocated sequentially including all CDR types.</td>
</tr>
<tr>
<td>Record extensions</td>
<td>Om</td>
<td>A set of network manufacturer specific extensions to the record. Conditioned upon the existence of an extension.</td>
</tr>
</tbody>
</table>
Subscriber and Equipment Tracing

- Subscribers or phones can be traced on request of law enforcement officials or for other reasons
- Search HLR + VLR
- Level-3 network messages are logged to the CDR for the duration of the trace for more precise localisation

Figure 1: Subscriber and Equipment Trace for 12.08
Plan of Presentation

• Introduction
  – What is cellphone localisation?
  – Why localise cellphones?
  – How do cellphones work, anyway?

• Cellphone localisation methods
  – What about GPS?
  – Radio Interface Techniques
  – Database Correlation Technique
  – Example of Database Correlation
  – Indoor Localisation
  – Hybrid method
  – Localisation in practice

• Demonstration
  – Examples of available data using a GSM trace mobile
Demonstration: GSM Trace Mobile

- Look at real time GSM Level-3 Messages
  - TEMS GSM 900 1800
  - Call setup
  - Authentication
  - Encryption
  - Network Measurement Reports
  - Handover
  - And so on…
Acknowledgements

• To Iness Ahriz and Yacine Oussar for help with the fingerprinting data analysis
Thank You.

Comments, questions?