

Programming Ubiquitous Things
2024/25 - Spring 2025 - UiO

Cellular-Based Systems

Prof. Paulo Ferreira
paulofe@ifi.uio.no
UiO/IFI/PT

© Paulo Ferreira



Contents

- Introduction and some basic definitions
- GPS and Differential GPS
- Infrared and Ultrasonic Location Systems
- Location Estimation with 802.11
- Cellular-Based Systems
- Other Approaches
- Location-Based Applications and Services
- Conclusions

© Paulo Ferreira



Cellular-Based Systems

© Paulo Ferreira

3

Cellular-Based Systems - Introduction



- The development of **location systems based on mobile phone technology** was originally driven by:
  - the U.S. Federal Communication Commission **E911** mandate, and
  - its European Community counterpart **E112** to locate mobile phone calls to assist in providing emergency services
- In addition, the wide adoption and ubiquitous connectivity of cellular phones makes them tempting platforms for the delivery of **location-based services**:
  - advertising, recommendation systems, and gaming
- A localization system based on cellular signals, such as GSM or CDMA, has the key advantages that:
  - it **leverages the phone's existing hardware**, and
  - can potentially provide **location estimates anywhere** voice service is available
- A number of mobile phone-based location systems have been developed, and they can be grouped into four categories:
  - **cell ID-based approaches / radio modeling / fingerprinting**
- Each type of location system has a different trade-off between:
  - **ease of deployment, coverage, and accuracy**

© Paulo Ferreira

4

Cellular-Based Systems – Cell ID-Based (1/2)



- A mobile-phone base station is typically equipped:
  - with a number of directional **antennas** that
  - define **sectors** of coverage or cells,
  - each of which is assigned a unique **cell ID**
- Cell ID-based location is a simple technique where:
  - the **position of the mobile phone is estimated based on the ID of the cell** currently providing service to the device
- Cell ID-based location is **usually implemented on the network side**, and its key advantage is:
  - it **works for all phones**, as **no handset modifications** are required
- **Accuracy depends on the size of the cell**, ranging:
  - from **150 m for microcells** in urban cores to **30 km for cells in rural settings**
- Such accuracy **may be sufficient for some applications**:
  - e.g., weather and traffic reports, but
  - falls short of the requirements for other application such as street navigation and the E911 guidelines (as these require a cell phone handset to be localized within 50 m 66% of the time)

© Paulo Ferreira

5

Cellular-Based Systems – Cell ID-Based (2/2)



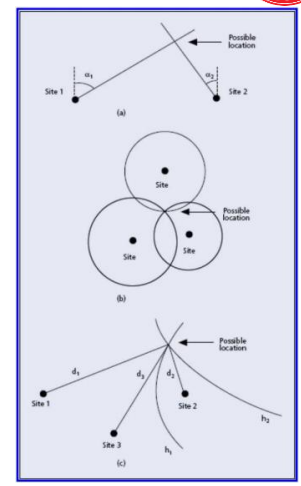
- The sytem by Laasonen is an example of a cell-ID based system:
  - it was **implemented purely on the handset** without network cooperation
  - it **monitors the ID of the cell the handset receives service from** and **uses the transition between cells to recognize the common places that a user goes to**
  - it **does not attempt to estimate absolute location**, but rather **assigns symbolic locations** (e.g., Home and Grocery Store)
  - **it does not need to know the coordinates of the cell towers**
  - the **privacy improvement in this "handset-only" approach is marginal, as current protocols require the mobile phone to register with the cell tower to obtain the cell ID**

© Paulo Ferreira

6

Cellular-Based Systems – Radio Modelling (1/6)

- A **variety of location systems based on modeling** of GSM and CDMA radio signals have been developed:
  - **most are based on time-of-flight measurements (rather than signal strength)**
- The **underlying techniques** used for computing ranges to cell towers **depend on the specifics of the GSM or CDMA** physical layer:
  - but the **positioning algorithms** used by GSM and CDMA are in fact **very similar**
- The main radio **modeling positioning methods** provided by GSM and CDMA systems are **based on Time Difference of Arrival** (**TDOA**) trilateration:
  - **handset position is estimated by intersecting hyperbolic lines** derived by taking **differences between time measurements from pairs of base stations**



intersection of two hyperbolic curves derived from measurements to three base stations:
- (a) angle of arrival;
- (b) time of arrival;
- (c) time difference of arrival

© Paulo Ferreira

7

Cellular-Based Systems – Radio Modelling (2/6)

- **TDOA requires base stations to be tightly synchronized**:
  - this is not an issue for CDMA networks (follow a synchronous protocol)
  - in GSM, this requires the deployment of additional network elements to determine the clock difference between base stations
  - this information is then provided to the **handset** who uses it to **calibrate the measurements from neighboring base stations**
- TDOA can be implemented either on the **network** or on the **client**
- Network-based approach:
  - three or more base stations **compare observations to determine the time differences** at which handset transmissions are heard at the cell towers
  - has the advantage that **it does not require modifications to the handset** hardware, and as a result, it works for existing, deployed handsets
- Client-based implementation:
  - the **handset measures the time differences in the arrival of training sequences** or pilot symbols transmitted by three or more cells
  - provides a **higher degree of privacy to users**, as time-difference is measured and the location estimated on the user's local device

© Paulo Ferreira

8

Cellular-Based Systems – Radio Modelling (3/6)

- TDOA **accuracy ranges between 50 and 500 m** depending on interference, system geometry, and multipath effects:
  - handsets in close proximity to a base station may suffer from **interference** issues where the strong signal of the nearby base station prevents the handset from hearing the transmission of neighboring nodes
  - this problem is more pronounced for CDMA systems, where different towers transmit on the same frequency, than on GSM networks, where towers are allocated different frequencies
  - to alleviate, base stations stop transmission for short idle periods that enable the handset to measure other neighboring nodes

- **Multipath effects**, resulting from signal reflecting on obstacles degrade the accuracy of the technique by lengthening the perceived distance to the base station

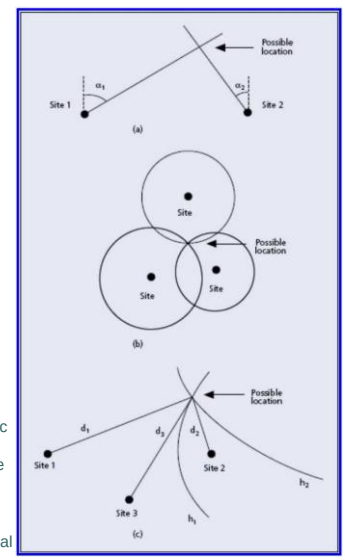
© Paulo Ferreira

9

Cellular-Based Systems – Radio Modelling (4/6)

- In addition to TDOA, GSM, and CDMA also provide positioning methods based on angle or arrival (AOA) and time of arrival (TOA)

- AOA is a method that determines position by electronically steering a directional antenna or an antenna array:
  - handset position is determined using triangulation, by intersecting a minimum of two directional lines of bearing



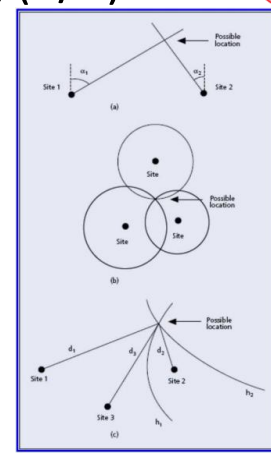
intersection of two hyperbolic curves derived from measurements to three base stations:
- (a) angle of arrival;
- (b) time of arrival;
- (c) time difference of arrival

© Paulo Ferreira

10

Cellular-Based Systems – Radio Modelling (5/6)

- The most significant drawback and advantage of AOA is:
  - it **requires specialized antennas and receivers**, which limits this approach to network-based implementations
  - it has the advantage that **it does not require system-wide synchronization** and is **more robust to multipath** propagation effects
- In **TOA**, the **handset position is determined by intersecting range circles**:
  - TOA systems can be implemented at **either the network or the client**
- A **significant downside of TOA** systems is that:
  - the **measuring device has to have accurate knowledge of the time of transmission** to determine the signal propagation time
  - that is why **TDOA systems get around this requirement by taking the difference between measurements**



intersection of two hyperbolic curves derived from measurements to three base stations:
- (a) angle of arrival;
- (b) time of arrival;
- (c) time difference of arrival

© Paulo Ferreira

11

Cellular-Based Systems – Radio Modelling (6/6)

- GSM and CDMA location systems based on the measurement of **received signal strength** have also been developed:
  - it is **less common than time-based approaches**, as it typically achieves lower performance
  - e.g., PlaceLab system, which complements their 802.11 signal models with a model that predicts tower distance based on received signal strength
- In Place Lab:
  - **cell tower locations are estimated using war-driving tools** similar to those used to estimate 802.11 base station locations
  - e.g., in three Seattle neighborhoods, **Place Lab achieved median accuracy between 100 and 200 m** depending on building and tower density; more densely populated neighborhoods, which tend to have a higher concentration of base stations, had better accuracy
  - the **handset-based approach** enables location determination **without the need for cooperation from the network operator** but requires the **mobile to store a database of tower locations**

© Paulo Ferreira

12

Cellular-Based Systems – Signal Strength Fingerprinting (1/2)

- Signal strength fingerprinting is an empirical location technique that involves:
  - a "training" or "mapping" phase in which a radio map of the environment is constructed by collecting a series of fingerprints in multiple location
- A radio fingerprint reflects some property, commonly as the signal strengths, of a group of radio sources that are heard at a specific location
- Once the training phase is complete:
  - **a client can determine its location by looking for the closest matches of the current measurement to the set of measurements collected in the training phase**

© Paulo Ferreira

13

Cellular-Based Systems – Signal Strength Fingerprinting (2/2)

- This solution is **very similar to the fingerprinting systems based on 802.11** but there are some differences:
  - due to higher coverage, cellular fingerprinting has the **potential to work in more places** than 802.11 fingerprinting
  - because cell towers are more dispersed across the covered area, a cellular-based localization system would **still work in situations where a building's electrical infrastructure has failed**
  - the significant expense and complexity of cellular base stations result in a network that **evolves slowly** and is only **reconfigured infrequently**
  - while this lack of flexibility (and high configuration cost) is certainly a drawback for the cellular system operator, **radio maps for cellular systems will degrade**
  - due to shorter range, **802.11 fingerprinting is more accurate** than cellular fingerprinting given the same number of radio sources

© Paulo Ferreira

14

Cellular-Based Systems – Comparison

- Location services: Cell-ID, TDOA, AoA, TOA, Fingerprinting
- Each of these types of location services strikes a different trade-off between:
  - ease of deployment, coverage, and accuracy
- Cell ID provides:
  - the lowest accuracy, but
  - because it does not require additional hardware on the network side, it is the one method that is universally supported by all network providers
- TDOA:
  - provides higher accuracy, but
  - because it requires changes to the network, the handset, or both, it is not yet universally supported

© Paulo Ferreira

15

Cellular-Based Systems – Comparison



Technology	GSM signal-strength fingerprinting	GSM TOF and signal-strength modeling	GSM/CDMA proximity
Accuracy	★★★☆ 2D coordinates with 4 m median accuracy in dense cell environment	★★☆☆ 3D coordinates with 100 - 200 m accuracy	★☆☆☆ Accuracy dependant on cell tower density (150 m – 30 km)
Coverage	★★☆☆ Building to campus scale. Requires cell network coverage and radio map. Best accuracy when 3+ cells are visible	★★★☆ Areas with GSM coverage and radio map. Best accuracy when 3+ cells are visible	★★★★ Anywhere with cell coverage and cell-to-location map
Infrastructure cost	★★★☆ No additional infrastructure is needed beyond cell network. Creating radio map is time intensive	★★★★ No additional infrastructure is needed beyond cell network and map of tower locations	★★★★ No additional infrastructure is needed beyond cell network and map of tower locations
Per-client cost	★★★★ Software only solution	★★★★ Software only solution	★★★★ Software only solution
Privacy	★★☆☆ Even if location is computed on client device, the network still tracks a handset's associated cell	★★☆☆ Even if location is computed on client device, the network still tracks a handset's associated cell	★★☆☆ Even if location is computed on client device, the network still tracks a handset's associated cell
Well-matched use cases	Asset and personnel tracking in indoor environments, indoor mapping/navigation/tour guides	Social networking, emergency response, neighborhood-scale information access, fitness tracking, outdoor mapping / navigation	Regional information access (weather, traffic, etc.)

© Paulo Ferreira

16