Location-Based Services

Petteri Nurmi
Questions

- How location-based services (LBS) operate and what kind of services there are currently available?
- What are E911 and E112?
- What are the main challenges for LBS?
- What is an inference attack on location data?
- What kind of countermeasures are available against inference attacks on location data?
- What are duty cycling and sensor management?
- What kind of tracking problems there are?
Location-Based Services (LBS)

- **Computer applications that deliver information depending on the location of the device and user**
  - Local or global: works in a specific environment (e.g., campus) vs. everywhere (e.g., GPS navigation)
  - Personal or collaborative: designed for single user (e.g., mobile maps) or multiple persons (e.g., participatory sensing)
- Typically require network access and infrastructure for measuring location information
  - Location determination topic of second week
Architecture of LBS - Stakeholders

- **Mobile client**
  - Runs the application/service on a mobile device
- **Location system**
  - Responsible for determining the location of the device
  - Position can be determined on the client or by infrastructure
- **Service provider**
  - Provides the application/service
  - E.g., advertising service
- **Content provider**
  - Provides content within the application/service
  - E.g., company that provides advertisements for the service
Lifecycle of LBS

1. Client requests the service for location sensitive information

2. Location system determines the location of the client (or uses latest estimate)

3. Request for information and current location sent to service provider that returns relevant information
   - Typically data connectivity needed
   - Optionally some information could be cached/stored on the client directly
Categories of LBS - Emergency Services

- **E911 (Enhanced 9-1-1)**
  - Locate where a call to an emergency number originates
  - Strict guidelines regarding positioning accuracy and consistency:
    - 50/100 meters 67% of times (handset/network-based)
    - 150/300 meters 90% of times (handset/network-based)

- **E112**
  - European equivalent of E911
  - No strict positioning requirements
    - “best effort” with respect to technological possibilities of infrastructure
Categories of LBS - Mobile Advertising

- Mobile marketing/advertising
  - One of the most popular domains for LBS currently
  - Push-based: advertisements delivered to the client terminal automatically
    - Permission-based: require user’s consent
  - Pull-based: client requests for advertisements
- Different location-sensitive advertising approaches:
  - Proximity-based: user’s within close proximity pushed advertisement
  - Profile-based: Routines detected by mining user’s location history
  - Coupons: discount vouchers delivered on the mobile device based on locations/shops visited (and profile)
Categories of LBS - Mobile Advertising

http://www.youtube.com/watch?v=8vPpyVXe4L0
Categories of LBS - Location-Based Games

• Game where the game play varies or evolves according to user’s location
  • Geocaching most prominent example
    • Treasure-hunt kind of game
    • User searches for boxes that other users have hidden
    • Boxes specified by coordinates
• Serious games
  • Games that aim to achieve some desirable objective
  • E.g., learning or achieving behavior change
  • Example: Savannah, a location-based game that teaches children behavior of lions
Categories of LBS - Location-Based Games

• Mixed reality games
  • Games that consist of a virtual and physical reality
  • Actions in the physical world affect the state of the game in virtual reality
  • Example: Can You See Me Now, urban chase game, performers on the street chase online (virtual) players
  • Example: PacLan / Pac-Manhattan: real-world versions of Pacman

• Urban games
  • Games that use the urban environment for gameplay
Categories of LBS - Location-Based Games

http://www.youtube.com/watch?v=3ozUNUTNMT4
Categories of LBS - Location-Based Games

http://www.youtube.com/watch?v=KJqxC9FbSCY
Categories of LBS - Mobile Augmented Reality

- Live, direct or indirect view of a physical real-world environment that is augmented with virtual content
- Common example: see-through lens + virtual content
- Location needed for two purposes:
  - Tracking the orientation and pose of the device (viewport that is being augmented)
  - Tracking the location of the client for delivering suitable information
- Wide range of examples especially for outdoors:
  - Tourist guides
  - Interactions at a distance (e.g., architecture)
Categories of LBS - Mobile Augmented Reality

http://www.youtube.com/watch?v=ZKw_Mp5YkaE
Categories of LBS - Navigation Systems

- System that assists people in the movement from one place to another
  - Indoors: supermarkets, malls, airports, campus or office environments
  - Outdoors: pedestrian navigation in cities or within large tourist sights
- Various ways to present route instructions
  - Mobile maps (2D or 3D)
  - Landmarks (verbal, auditory, visual, multimodal)
    - Generally considered most effective way to present navigation instructions for pedestrian purposes
Categories of LBS - Navigation Systems

http://www.youtube.com/watch?v=IXt21v8Hjhw
Categories of LBS - Mobile Tourist Guides

- Mobile systems that provide assistance to tourists visiting a particular city or other location
  - Cyberguide and Guide from previous lectures are examples of early prototypes of these systems
- Common functionalities include
  - Map with information about interesting locations
  - Navigation support
  - Location-sensitive recommendations
- Also other variations:
  - E.g., restaurant or other point-of-interest (POI) finders
Categories of LBS - Mobile Tourist Guides

http://www.youtube.com/watch?v=hAcAHgUge-8
Categories of LBS - Participatory Sensing

• The concept of communities contributing sensory information to form a body of knowledge
  • Mapping prices at different gas stations
  • Nericell: mapping road conditions in India

• Active research area currently, examples of topics:
  • Providing suitable incentives to participate in data collection
  • Security and privacy
  • Determining which users to ask to contribute to data collection
Categories of LBS - Participatory Sensing

http://www.youtube.com/watch?v=t-lfpa3XiY
Other categories of LBS

- Mobile media
  - Tag and retrieve content (photos, videos, music) based on location
- Social networking
  - Get notifications when a friend is in close proximity
  - See locations of friends on a map
- Location-Based Recommenders
  - Obtain recommendations about interesting places, restaurants, etc. that are near current location
  - Get information about friends that have visited a particular location before
Challenges in LBS

- Lack of standards
  - Phone manufacturers have different APIs
  - Location-sensitive databases have different formats
- Positioning
  - Tradeoff between power consumption and accuracy
  - Lack of widely available indoor positioning solution
- Power consumption
  - Sensing (including positioning) and Internet connectivity have high power consumption
- Privacy
  - Possibility to deduce sensitive personal information
Location Privacy

Ability to prevent other parties from learning one’s current or past location

Beresford & Stajano, 2003

Special type of information privacy which concerns the claim of individuals to determine for themselves when, how and to what extent location information about them is communicated to others

Duckham & Kulik, 2006
Location Privacy – Inference Attack

- An approach that aims to discover sensitive private information from location data
  - Detect patterns in location data
  - Cross-correlate patterns with other data sources
- Home and workplace detection
  - Place detection (discussed on week 5) can be used to identify places where person stays regularly
  - Correlations with time can be used to determine home and workplace for over 80% of individuals
  - Home address detection also examined in the context of GPS traces from drivers
Location Privacy – Inference Attack

- Gruteser and Hoh: completely anonymized GPS data from multiple (3 and later 5) users
  - Clustering can be used to reconstruct original traces of each user with high accuracy despite anonymization
- Wilson and Atkeson: Presence sensors within a smart home (motion detectors, pressure mats, …)
  - Observations from any single sensor not sufficient for detecting identity
  - Patterns in sensor triggering sequences could be used to determine who in the house was where (around 85% accuracy)
Location Privacy – Countermeasures

2. Privacy policies: trust-based agreements between individuals.
3. Anonymity: use a pseudonym or create ambiguity by grouping people together.
4. Obfuscation: reduce the quality of location information.

- First two are manual enforcement techniques
- Last two are computational privacy measures
Location Privacy – Anonymity

- Basic idea to replace associated name with a pseudonym or other untraceable identifier
  - Naïve approach: change pseudonyms regularly to reduce risk of learning about habits
    - Clustering can be used to detect which pseudonyms belong together, at least when data from only few individuals
- k-Anonymity
  - Instead of reporting the location of a person, report a region containing k-1 people
    - Additional information, such as patterns in service requests, could be used to break k-anonymity
    - “Historical k-anonymity”: inject ambiguity into additional information as well
Location Privacy – K-Anonymity

- The protection provided by k-anonymity sensitive to
  - Choice of the value of k
  - The positions of the entities

- K-anonymity can be extended to protect the identify of the person who initiated location request
Location Privacy – Mix Zones

- Application zones:
  - Areas where location-based services are used
  - User’s location reported
- Mix zones
  - Areas between the application zones
  - User given a new, unused pseudonym when transferring from application zone to mix zone
Location Privacy – Spatial and Temporal Degradation

• Alternative countermeasure is to degrade the quality of location measurements
• Adding white noise to measurements
  • Random samples from a zero-mean Gaussian
  • Standard deviation determines extent of noise
Location Privacy – Spatial and Temporal Degradation

- Temporal degradation:
  - Increasing time between location reports
- Cloaking
  - Removing data from certain locations (spatial) and/or from certain times (temporal)
Continuous sensing and reporting of locations consumes significant amounts of energy.

Approaches for sensing location vary significantly in terms of power consumption:
- Typically: GPS > WiFi > Accelerometer > GSM

Three ways to reduce power consumption:
- Reduce sensing frequency (duty cycling)
- Use low-power sensors whenever possible (sensor management)
- Reduce reporting frequency (intelligent data uploading)
Energy-Efficiency

- Savings in power consumption often come at the expense of positioning accuracy
- Potential solution is to optimize error consumption for a given error threshold $E$
  - Reduce power consumption as much as possible
  - Guarantee that position error never (or seldom) exceeds the error threshold $E$
- Monitoring of location related information referred to as *tracking*
Energy-Efficiency – Tracking

- Position tracking:
  - Estimate and report new position only when position error cannot guaranteed to be within error threshold
  - Can be understood as a circle of uncertainty around the last reported location

- Trajectory tracking:
  - Report information about the user’s trajectory when error of the trajectory exceeds a threshold
  - Error corridor around actual trajectory

- Buddy tracking:
  - Report entrance/departure of a friend from close proximity
Formally duty cycle is defined as the ratio of the duration of the event to the total period:

\[ D = \frac{T}{\tau} \]

- Sampling rate
  - Number of measurements taken in unit time (seconds)
  - For example, 90Hz = 90 measurements per second

- Duty cycling:
  - Reduce the sampling rate by keeping the sensor idle
  - Example: measurements collected for one second during a 10 second window \( \Rightarrow \) duty-cycle 0.1
Energy-Efficiency – Duty Cycling

- GPS usage can be reduced by estimating the time that is needed to reach a point that violates error threshold
  - Assume constant velocity over a data window
  - Schedule next GPS measurement using
    - Estimated error reflects the estimated distance that user has moved since last measurement

\[ 
\Delta t = \min(\frac{E_{Position}}{V_{est}}, \frac{E_{Trajectory}}{V_{est}}) - e_{model} \]

- Estimated error since last position update
- Estimated speed of the user
Energy-Efficiency –
Sensor Management

• Reduce power consumption by using low power sensors when possible

• Most common example is to use accelerometer to detect motion instead of continuous GPS sampling
  • Assume constant velocity \( v \), distance from previous location \( s = vt \)
    \[\Rightarrow\] no need to sense position if duration of motion < \( E/v \)
  • Motion typically detected using the total variance of accelerometer axes over a window
Energy-Efficiency – Sensor Management

- Compass heading can be used to reduce need for GPS when user is moving along a straight line
  - Assume constant velocity
  - Position estimated using accumulated orthogonal distance (discussed later during the course)
  - Position update triggered when error estimate exceeds the tracking threshold

\[ D_{orth}(t_k) = \sum_{i=1}^{k} (t_i - t_{i-1})S_{gps}sin(||\theta_{start} - \theta_i||)(1 + \sigma) \]
Energy-Efficiency – Data Uploading

- Data uploading protocol defines when measurements are sent to a server
- Position tracking:
  - Let $x$ denote the last measurement sent to a server
  - Let $y$ denote a new GPS measurement
  - Send measurement to server if $d(x,y) > E$, i.e., error threshold violated
- Trajectory tracking:
  - Trajectory simplification used to select a subset of points that allow reconstructing the original path sufficiently accurately
    - More on this during week 5
Energy-Efficiency – Buddy Tracking

- Trigger update (or alert) whenever another user (or friend) comes (or leaves) the vicinity of an user

- Strips algorithm
  1. Exchange location messages between devices
  2. For each pair of devices \((a,b)\), determine a strip \(S(a,b)\) along which all points are equally far from \(a\) and \(b\)
  3. If \(a\) or \(b\) violate the strip \(S(a,b)\), they exchange location information
     - If within close vicinity, trigger entrance
     - If not within close vicinity, redefine the strip \(S(a,b)\)
Energy-Efficiency – Buddy Tracking
Summary

- Location-based services
  - Computer applications that deliver information depending on the location of the user and/or device
  - Require access and to network and location information
  - Client, location system, service provider, content provider
- Location privacy
  - Privacy that concerns ability to determine when, how, and to which extent location information is communicated
- Location Inference attack
  - Computational approach that attempts to discover sensitive personal data from location traces
Summary

- Computational countermeasures
  - Anonymity: k-anonymity, mixed zones
  - Obfuscation: cloaking, noising, temporal degradation
- Energy-efficiency
  - Duty cycling: reducing sampling rate
  - Sensor management: using low power sensors when possible
  - Uploading policies: reduce time span when location reported
- Tracking: position, trajectory and buddy tracking
Literature – Location-Based Services


Literature – Location-Based Services


Literature – Computational Location Privacy

- Hoh, B.; Gruteser, M.; Xiong, H. & Alrabady, A.
Literature – Energy-Efficiency


