Mobile Positioning vs. Privacy

Mikko Heikkinen
undergraduate student
Networking Laboratory
Helsinki University of Technology
mikko.heikkinen(at)hut.fi

3.11.2004

Outline

- 1 Introduction
  - 1.1 Technical Background
- 2 Legislation
  - 2.1 Legislation in the EU
    - 2.1.1 Case Finland
  - 2.2 Legislation in the USA
- 3 Privacy Enhancing Technologies
  - 3.1 Mix Networks
  - 3.2 P3P
  - 3.3 Intermittent Connectivity
  - 3.4 User Interface Solutions
  - 3.5 Trusted Location Cloaking Proxy
- 4 Discussion and Conclusions

1 Introduction

- brings a myriad of privacy issues
- enables finding of the current location of a specific mobile phone or other suitable mobile device
- can be used to implement various safety, billing, information, and tracking services

1 Introduction (2)

Table 1: Examples of Mobile Positioning Services

Application	Mass acceptance accuracy requirements	Objective	Location frequency
Location Sensitive Billing	250m	Competitive Pricing	Originated calls, received calls, mid-call
Roadside Assistance	125m	Send help	Originated calls
Mobile Yellow Pages	250m	What's near me?	Originated calls
Traffic information	Cell/Sector	What's traffic like?	Originated calls or every 5 min
Location based messages	125m	Advertise, alert, inform	Originated calls or every 5 min
Fleet tracking	30 - 125m	Resource management	Every 5 min or on demand
Track packages	Cell/Sector	Locate and direct	On demand
Driving directions	30m	Guidance	Every 5 secs

1.1 Technical Background

- Cell of Origin (COO)
  - the location of a mobile device is the location of the base station the device is currently using
  - in urban areas an accuracy of 150 metres can be reached within pico cell sites
  - the accuracy decreases rapidly when larger cell sizes are in use
  - a response time of three seconds
  - can be deployed without modifications to mobile devices

1.1 Technical Background (2)

- Enhanced Observed Time Difference (E-OTD)
  - based on calculating time differences in signal arrival between at least three base stations and a location measurement unit
  - calculation is done by mobile devices enabled with E-OTD software
  - provides accuracy between 50 and 125 metres
  - a response time of five seconds
  - requires software modifications on existing mobile phones

1.1 Technical Background (3)

- Time of Arrival (TOA)
  - requires the time synchronization of base stations with GPS or atomic clocks
  - quite expensive to implement
  - does not require modifications to mobile devices
  - offers slightly better accuracy than COO
  - has a slow response time around ten seconds making it unusable for many applications

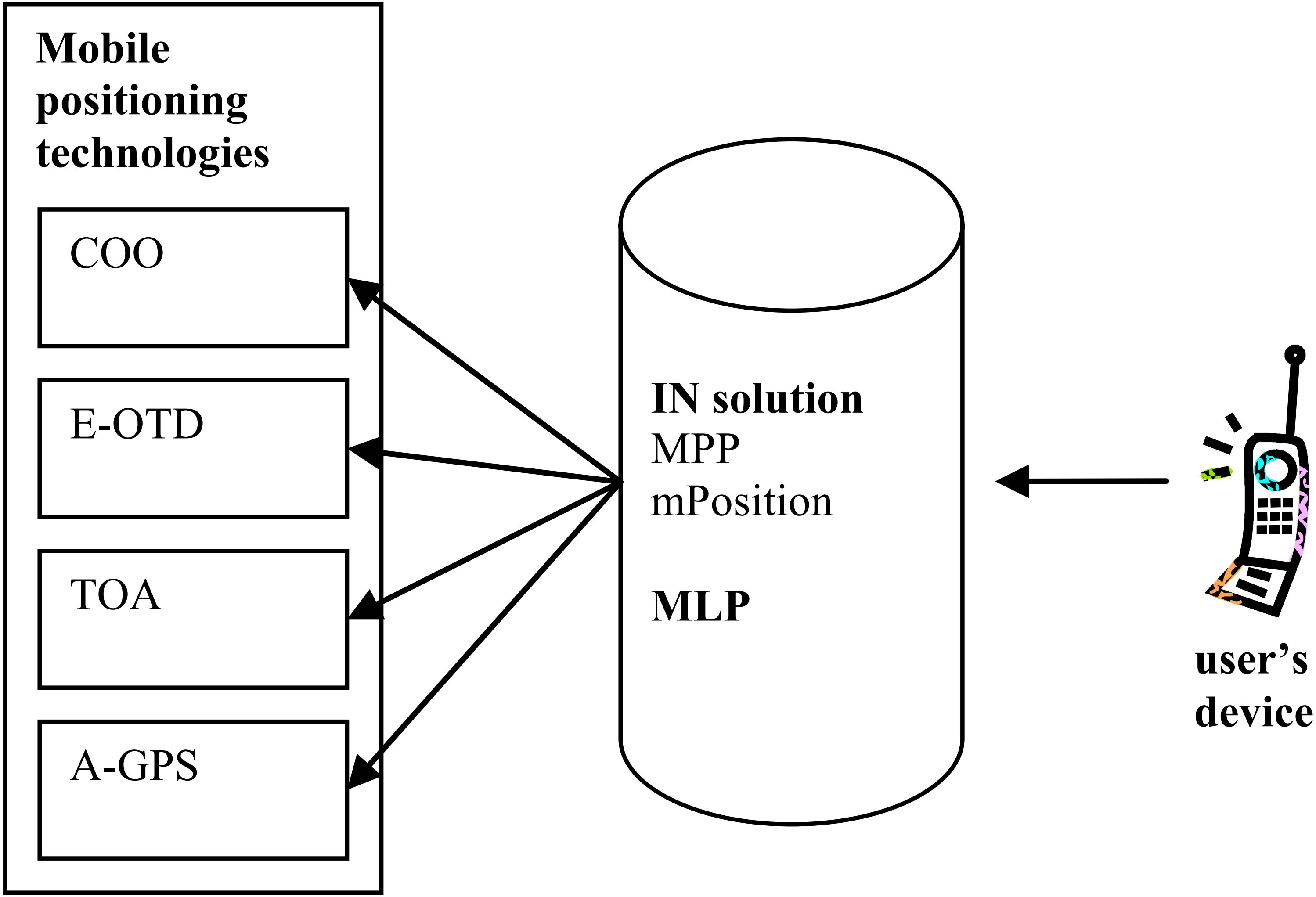
1.1 Technical Background (4)

- Assisted GPS (A-GPS)
  - uses the Global Positioning System (GPS) to derive the location information
  - best results when mobile network shares the calculation with the mobile device
  - requires A-GPS enabled mobile devices
  - an accuracy of around 20 metres
  - a response time of a few seconds
  - expensive to implement

1.1 Technical Background (5)

- Intelligent Network (IN)
  - Mobile Positioning Protocol (MPP) by Ericsson
  - mPosition by Nokia
  - a mobile location center
    - relays the location information from lower level protocols to the application requesting the information
- Open Mobile Alliance's Mobile Location Protocol (MLP)
  - tries to establish vendor independent location messaging
  - requires that both the location center providing the location information and the location based service requesting it comply with MLP's XML based messaging

1.1 Technical Background (6)



Mobile positioning technologies

COO

E-OTD

TOA

A-GPS

IN solution
MPP
mPosition

MLP

user's device

1.1 Technical Background (7)

- MobileIP
  - enables an IP node to roam freely in different IP based networks while maintaining its home IP address
  - terminology:
    - a mobile IP node
    - home IP address
    - a home agent
    - care-of-address
  - IPv6 provides route optimization capabilities

2.1 Legislation in the EU

- European Union directive 2002/58/EC
  - officially adopted on July 12, 2002
  - establishes a common framework for data protection in telecommunication services and networks
    - regardless of the technology in use
  - differentiates between
    - location data *within* traffic data giving less precise positioning information
      - informed consent is required when location information is used for value added services
    - location data *other than* traffic data allowing the exact positioning of user’s device
      - either anonymisation or informed consent is required
      - *and* users that have given their consent have the possibility to temporarily refuse the processing of location information for each connection or transmission of a communication

2.1.1 Case Finland

- directive 2002/58/EC was implemented in the privacy law concerning electronic messaging (SVTSL 516/2004) on September 1, 2004
- a telecom operator is entitled to use location information if its customer has not prohibited it to do so
- operator must get an agreement from its customer before it is allowed to give away location information to a third-party service provider
  - for each service separately
- allows the use of location information for telecom operators in order to provide value added services
  - each customer has the right to deny the use of his or her location information for these purposes

2.2 Legislation in the USA

- much looser compared to the EU
- no established general data protection
- industry has developed privacy regulation in a self-regulated way
- certain governmental parties interested in privacy regulation
  - Federal Trade Commission (FTC)
  - Federal Communications Commission (FCC)
- FCC ruled on July 24, 2002
  - wireless carriers must receive a customer's explicit approval before using their location information
  - situation seems clear but the liberal nature of American legislation always paves way for trials
- specific issues
  - Children’s Online Privacy Protection Act
    - prohibits the collection of private data online from children without prior consent from their parents
  - E911 legislation
    - position of emergency callers to authorities
    - nation-wide emergence of positioning capabilities

3 Privacy Enhancing Technologies

- many risks involved when mobile positioning is being used:
  - financial risks
  - spam
  - harm to reputation
- solutions:
  - 3.1 Mix Networks
  - 3.2 P3P
  - 3.3 Intermittent Connectivity
  - 3.4 User Interface Solutions
  - 3.5 Trusted Location Cloaking Proxy

3.1 Mix Networks

- a pseudonymous IP network
- privacy protection by hiding user’s actual IP address and other personally identifying information
- Anonymous Internet Proxies (AIPs)
  - core network privacy daemons
  - pass encapsulated packets between themselves
  - traffic between AIPs is symmetrically encrypted

3.2 P3P

- originally established as a standard to control privacy preferences in web services
  - based on the XML language
- used in conjunction with the MobileIP
  - home agent
    - needs to have a web server interface and a privacy policy set up
    - mobile users can grant or revoke their consent to use location based information using the web interface
  - mobile node
    - has to have a P3P-compatible user agent including P3P privacy preferences
    - accesses the home agent’s web site in order to receive the current privacy policy set by the user
- problems:
  - when the mobile node negotiates with the home agent about the privacy policy, it actually sends information about its current location
    - home agent must be inside a safe zone or anonymous connections have to be allowed
  - user cannot be sure whether third-party value added services actually obey his or her privacy policy
    - P3P must be backed up with binding legislation

3.3 Intermittent Connectivity

- mobile device avoids to reveal its precise position by requesting geographically coded requests *one set at a time* rather than individually through separate queries
- a user wants to know what kind of service is available on a specific address
    - requests what services are available on all addresses on the street
    - not just the specific address user is interested
- only suitable to a restricted group of applications
    - unnecessary additional data transfer

3.4 User Interface Solutions

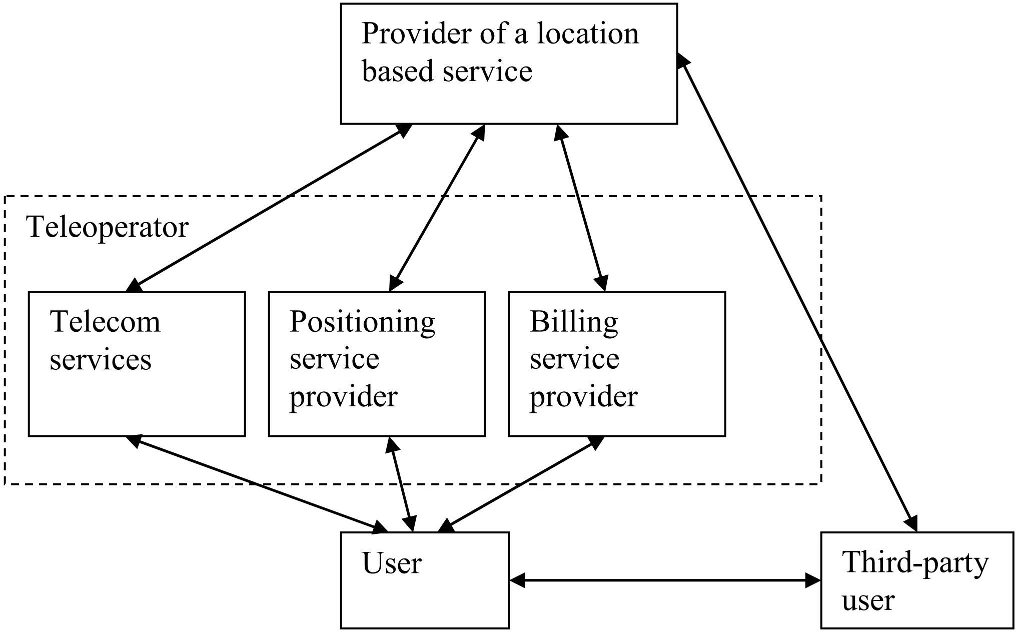
- innovative user interface design
- interface informs user
  - what extend user is giving away his location at the moment
  - who are requesting information about user’s location
- a certain balance has to be maintained
  - not to overload the user with unnecessary information

3.5 Trusted Location Cloaking Proxy

- adjusts the resolution of the location information reported to services based on the density of users in a region
- a user with k-anonymity
  - proxy runs a cloaking algorithm that selects the smallest of a set of regions that includes the user and at least k-1 other users
    - reports it to the service
  - the distrusted service cannot easily map the reported location back to an individual user

4 Discussion and Conclusions

- many parties involved



4 Discussion and Conclusions (2)

- All parties
  - must comply with the privacy policies set by the law and by them themselves
  - must implement necessary security measures to prevent the abuse of location information
  - should avoid the unnecessary use of location information to prevent possible abuse
- All users
  - should be aware that their location information is being processed
  - should be always able to disallow such usage
  - should know precisely the extent and the purpose of location information processing

4 Discussion and Conclusions (3)

- who is the owner of user’s position?
  - current legislation provides no clear single answer
  - location information is somewhat analogical to portable mobile numbers
    - teleoperator maintains the number or position
    - the decision of its usage remains to the user
    - position is a much more abstract concept than number
      - increased flexibility and options in its usage causing greater risks of abuse
  - normal end-user will have substantial difficulties in trying to piece together all the different contexts and applications in which his or her location information might be used
  - though the user has a right to choose, he or she might not be able to gather sufficient information to make an informative decision

4 Discussion and Conclusions (4)

- legislation cannot do miracles
- the real hope lies in the goodwill of teleoperators and service providers
- the adaptation of positioning-based services will be severely hindered if there are substantial privacy scandals reaching critical amount of publicity
- a mutual respect of privacy will most likely guarantee a successful future for the promising positioning-based applications