

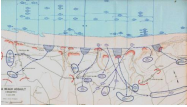
Location Privacy

Computer Science and Engineering - University of Notre Dame


Subtleties of Location Privacy

“... a 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, M. and L. Kulk, Location privacy and location-aware computing, in *Dynamic & Mobile GIS: Investigating Change in Space and Time*, J. Drummond, et al., Editors. 2006, CRC Press: Boca Raton, FL, USA, p. 34-51.



When: For D-Day attack, troop location privacy not important 70 years later







How: Alert fires to tell your family whenever you stop for pancakes




“Michael Michers Chocolates”
“Weight Watchers”
To what extent: Accuracy high enough to distinguish?

Computational Location Privacy


- Law – Privacy regulations enforced by government 
- Policy – Trust-based, often from institutions 
- Encryption – Applies to any type of data. 
- Computational Location Privacy – Exploits geometric nature of data with algorithms 

Why Reveal Your Location?

If you want to know your location, sometimes have to tell someone else.




Loki 2.0
Free location based search and navigation tool.
Loki Search, Find Me, Local Channels



QUOVA
Reverse IP


Loki Wi-Fi locator – send your Wi-Fi fingerprint and get back (lat, long)

Quova Reverse IP – send your IP address and get back (lat, long)




UbiSense – static sensors receive UWB to compute (x,y,z)

Exceptions




Cricket – MIT




POLS – Intel Research

Variable Pricing




Congestion Pricing

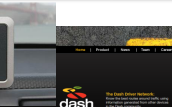



Pay As You Drive (PAYD) Insurance

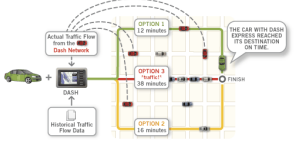
Traffic Probes



<http://dash.net/>







Routing The Dash Way
Dash was built from the ground up to be smart about traffic. Each Dash unit comes loaded with a database of historical traffic conditions for major metropolitan areas. Dash knows how fast traffic flows for every time and day of the year. Dash investigates this historical information along with traffic flow information sent from the network of other Dash devices to provide users up to 2 routing options. Finally a solution that gives you routing options based on real world conditions!

Social Applications

Dodgeball

Geotagged Flickr

Geotagged Twitter

MotionBased

The slide titled "Social Applications" features a red header bar. Below it, four screenshots are arranged in a 2x2 grid. Top-left: Dodgeball app interface showing a group of people. Top-right: Flickr map with red location pins. Bottom-left: Twitter map with red location pins. Bottom-right: MotionBased app interface showing a map and a graph.

Location-Based Services

Navigation

Local Information

Tracking

Games

Location Alerts

The slide titled "Location-Based Services" features a red header bar. Below it, five images are arranged in a grid. Left: A PDA-style navigation device. Top-center: A hand holding a smartphone. Top-right: A blue tracking device with a text box titled "A dingo-tracking device". Bottom-left: A person playing a game on a handheld device. Bottom-center: A screenshot of a location alert notification. Bottom-right: A small image of a book titled "Journal of Location Based Services".

Research

OpenStreetMap (London)

MSMLS (Seattle)

The slide titled "Research" features a red header bar. Below it, two maps are shown side-by-side. Left: OpenStreetMap of London, showing a dense network of white lines on a black background. Right: MSMLS of Seattle, showing a dense network of blue lines on a light background.


People Don't Care about Location Privacy

- 74 U. Cambridge CS students
• Would accept £10 to reveal 28 days of measured locations (£20 for commercial use) ⁽¹⁾
- 226 Microsoft employees
• 14 days of GPS tracks in return for 1 in 100 chance for \$200 MP3 player
- 62 Microsoft employees
• Only 21% insisted on not sharing GPS data outside
- 11 with location-sensitive message service in Seattle
• Privacy concerns fairly light ⁽²⁾
- 55 Finland interviews on location-aware services
• "It did not occur to most of the interviewees that they could be located while using the service." ⁽³⁾


⁽¹⁾ Danezis, G., S. Lewis, and R. Anderson. How Much is Location Privacy Worth? in Fourth Workshop on the Economics of Information Security, 2005. Harvard University, 2005.

⁽²⁾ Iachello, G., et al. Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. in Ubicomp 2005: Ubiquitous Computing, 2005. Tokyo, Japan.


⁽³⁾ Kaasinen, E., User Needs for Location-Aware Mobile Services. Personal and Ubiquitous Computing, 2003. 7(1): p. 70-79.



Documented Privacy Leaks



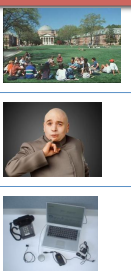
- How Cell Phone Helped Cops Nail Key Murder Suspect - Secret "Prings" that Gave Bouncer Away**
New York, NY, March 15, 2006
- Stalker Victims Should Check For GPS**
Milwaukee, WI, February 6, 2003
- Real time celebrity sightings
<http://www.gawker.com/stalker/>
- A Face Is Exposed for AOL Searcher No. 4417749**
New York, NY, August 9, 2006



Panel 1: A person says, "WELL, WE'RE ALMOST BACK TO MY PLACE."
Panel 2: A person says, "THANKS FOR THE DATE. I CAN MAKE IT FROM HERE."
Panel 3: A person says, "TO BETTER ATTACK THE TRACKING DEVICE, I'LL RUN DOWN THAT ALLEY AND HIDE UNTIL HE LEAVES."

Subtleties of Location Privacy


- Interviews of location based services users
• Less worry about location privacy in closed campus ⁽¹⁾
- Interviews in 5 EU countries
• Price for location varied depending on intended use ⁽²⁾
- Greeks significantly more concerned about location privacy
• Study two months after wiretapping of Greek politicians ⁽²⁾




⁽¹⁾ Barkhuus, L., Privacy in Location-Based Services: Concern vs. Coolness, in Workshop on Location System Privacy and Control, Mobile HCI 2004, 2004: Glasgow, UK.

⁽²⁾ Curtek, D., et al., A Study on The Value of Location Privacy, in Fifth ACM Workshop on Privacy in the Electronic Society, 2006, ACM, Alexandria, Virginia, USA, p. 309-318.

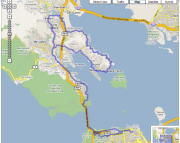
Computational Location Privacy Threats



Not computational:
stalking, spying, peeping




Not computational:
browsing geocoded images



Not computational:
browsing GPS tracks

Significant Locations From GPS Traces




comMotion (Marmasse & Schmandt, 2000)

- consistent loss of GPS signal → salient location
- user gives label (e.g. "Grandma's")

Ashbrook & Starner, 2003

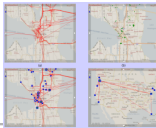
- cluster places with lost GPS signal
- user gives label

Common aim: find user's significant locations, e.g. home, work



Project Lachesis (Hariharan & Toyama, 2004)

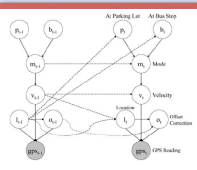
- time/space clustering
- hierarchical



Kang, Welbourne, Stewart, & Borriello, 2004


- time-based clustering of GPS (lat, long)

Context Inference




Patterson, Liao, Fox & Kautz, 2003

- GPS traces
- Infer mode of transportation (bus, foot, car)
- Route prediction



Location says a lot about you



Krumm, Letchner & Horvitz, 2006

- Noisy GPS matched to road driven
- Constraints from speed & road connectivity

Predestination (Krumm & Horvitz, 2006)

- Predict destination
- Extends privacy attack into future

Context Inference - Wow

Inferring Location Via Properties Based on User Location History
 Location history and location history analysis
 Location history and location history analysis
 Location history and location history analysis




Figure 3: Sensor allocation map for a part of the fourth floor.

Indoor location sensors

Machine learning to infer these properties based only on time-stamped location history

Table 1: User properties


USER PROPERTY	PROPERTY
ADE	gender: 'M', height: '58-74', weight: '150-250'
POSITION	gender: 'M', height: '58-74', weight: '150-250'
TEAM	gender: 'M', height: '58-74', weight: '150-250'
WORK	gender: 'M', height: '58-74', weight: '150-250'
FREQUENCY	gender: 'M', height: '58-74', weight: '150-250'
COPYRIGHT	gender: 'M', height: '58-74', weight: '150-250'
REVISION	gender: 'M', height: '58-74', weight: '150-250'
ROOM	gender: 'M', height: '58-74', weight: '150-250'
CONNECTIVITY	gender: 'M', height: '58-74', weight: '150-250'

IJCAI 2007

Location is Quasi-Identifier

Protecting Privacy Against Location-based Personal Identification
 "Check Name" - "New York" - "New York" - "New York"

Quasi-identifier – "their values, in combination, can be linked with external information to reidentify the respondents to whom the information refers. A typical example of a single-attribute quasi-identifier is the Social Security Number, since knowing its value and having access to external sources it is possible to identify a specific individual."



Secure Data Management, VLDB workshop, 2005

Simulated Location Privacy Attack 1


Location Privacy in Pervasive Computing

Active BAT indoor location system

Experiment

- Attach pseudonym to each person's location history
- Check
 - Where does person spend majority of time?
 - Who spends most time at any given desk?
- Found correct name of *all* participants


IEEE Pervasive Computing Magazine, Jan/March 2003

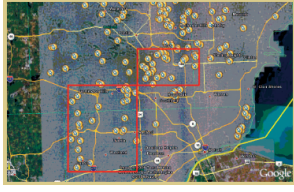


Simulated Location Privacy Attack 2

Enhancing Security and Privacy in Traffic-Monitoring Systems

IEEE Pervasive Computing Magazine, Oct/Dec 2006






Experiment

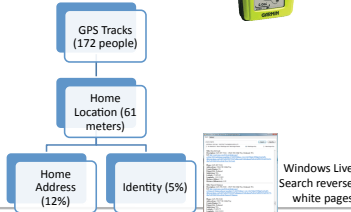
- GPS histories from 65 drivers
- Cluster points at stops
- Homes are clusters 4 p.m. – midnight
- Found plausible homes of 85%

Simulated Location Privacy Attack 3

Inference Attacks on Location Tracks

Pervasive 2007

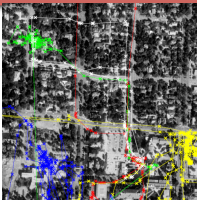




Simulated Location Privacy Attack 4


On the Associativity of Periodic Location Samples

Security in Pervasive Computing, 2005



From "multi-target tracking" algorithms originally designed for military tracking

- Three GPS traces with no ID or pseudonym
- Successful data association from physical constraints



Simulated Location Privacy Attack 5

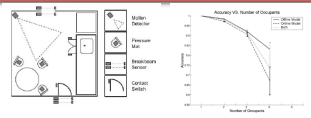
Smelliness Tracking & Activity Recognition (STAR) Using Tiny AreaSensors, Smart Sensors

David Wiltschko & Chris Athanasiadis
 Intel Research, Cambridge, MA, USA
 Intel Research, Berkeley, CA, USA
 Intel Research, Santa Clara, CA, USA

Abstract: In this paper we describe the Smelliness Tracking and Activity Recognition (STAR) system. STAR is a system that uses tiny area sensors to track the movement of people in a home. STAR is designed to be used in a home with three occupants and two state sensors. STAR is designed to be used in a home with three occupants and two state sensors. STAR is designed to be used in a home with three occupants and two state sensors.

1. Introduction


Advances in mobile devices and an increasing number of people are using location-based services. These services are designed to help users find nearby points of interest, such as restaurants, gas stations, and other services. These services are designed to help users find nearby points of interest, such as restaurants, gas stations, and other services.



Accuracy vs. Number of Occupants

Number of Occupants	Accuracy (%)
1	~95
2	~85
3	~75

- Home with three occupants
- Two-state sensors
- Continuity analysis on thousands of sensor readings
- 85% correct data association



Pervasive, 2005



Simulated Location Privacy Attack 6

A spatiotemporal model of strategies and counter-strategies for location privacy protection

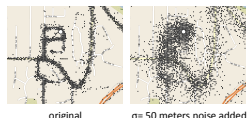
Mark DeGroot, Leo Kulkarni, and Arindam Bose
 Department of Computer Science, Stanford University, Stanford, CA, USA
 Department of Computer Science, Stanford University, Stanford, CA, USA
 Department of Computer Science, Stanford University, Stanford, CA, USA

Abstract: This paper presents a model of location privacy protection strategies and counter-strategies. The model is based on a spatiotemporal graph of locations and movements. The model is based on a spatiotemporal graph of locations and movements. The model is based on a spatiotemporal graph of locations and movements.

1. Introduction

Location privacy is a general type of privacy protection that concerns the ability of a user to control the information that is shared about their location. Location privacy is a general type of privacy protection that concerns the ability of a user to control the information that is shared about their location. Location privacy is a general type of privacy protection that concerns the ability of a user to control the information that is shared about their location.

Refinement operators for working around obfuscated location data



original $\sigma = 50$ meters noise added

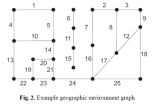


Fig. 2. Example geographic environment graph

Example refinement sources


- Must stay on connected graph of locations
- Movements are goal-directed
- Maximum speed constraint

GIScience 2006



Where Do You Want to Go Today?




We already know, more or less.



UbiComp 2006, The Eighth International Conference on Ubiquitous Computing, September 17-21, 2006, San Jose, CA, USA

Predestination: Inferring Destinations from Partial Trajectories

John Krumm and Eric Horvitz
 Microsoft Research
 One Microsoft Way
 Redmond, WA, USA 98002
 {jkrumm, horvitz}@microsoft.com

Efficient driving likelihood

- Clues to destination
- Previous destinations
- Ground cover
- Efficient driving
- Trip time

Accuracy = 2 km median error at halfway point of trip



How Do You Want to Get There?

Copyright © 2008 SAE International

Paper Number 08AE-101
A Markov Model for Driver Turn Prediction
 John Krumm
 Microsoft Research

Predict next road segments based on past road segments (Markov model)

Prediction Accuracy vs. Road Segments Predicted

(Each road segment is 237.5 meters (0.15 miles))

Road Segments Predicted into Future	Experimental Result	Random Guess (direction known)	Random Guess (direction unknown)
1	0.95	0.50	0.33
2	0.85	0.40	0.25
3	0.75	0.30	0.18
4	0.65	0.25	0.15
5	0.60	0.20	0.12
6	0.55	0.18	0.10
7	0.50	0.15	0.08
8	0.48	0.14	0.07
9	0.45	0.13	0.06
10	0.43	0.12	0.05

Full Route Prediction

Copyright © 2008 SAE International

Paper Number 08AE-283
Route Prediction from Trip Observations
 Jon Froehlich
 University of Washington
 John Krumm
 Microsoft Research

Average
Current Route
No Repeat Trips

1) Relatively small number of routes make up large fraction of drivers' trips

2) Cluster observed trips into repeated routes

3) Predict based on current trip's nearest historical route

Correct prediction of repeat trips by other drivers

Correct Trip Distance (km)

Top Match Within Top 2 Matches Within Top 5 Matches Within Top 10 Matches

Computational Countermeasures

3

Location privacy and location-aware computing

Matt Duckham & Lars Kolik
University of Melbourne, Australia

CONTENTS

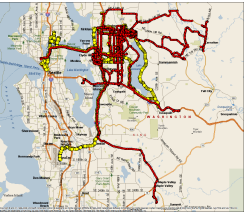
- 1.1 Introduction
- 1.2 Background and definitions
- 1.3 Positioning systems and location privacy
- 1.4 Location privacy protection strategies
- 1.5 Conclusions
- 1.6 Acknowledgements
- References

Dynamic & Mobile GIS: Investigating Change in Space and Time, CRC Press, 2006

Four ways to enhance location privacy

1. **Regulations** – gov't. enforced
2. **Policies** – trust-based agreements
3. **Anonymity** – pseudonyms and/or ambiguity
4. **Obfuscation** – reduce quality of data

Computational Countermeasures: Pseudonyms





Pseudonymity

- Replace owner name of each point with untraceable ID
- One unique ID for each owner

Example

- "Larry Page" → "yellow"
- "Bill Gates" → "red"






• Beresford & Stajano (2003) propose frequently changing pseudonym


• Gruteser & Hoh (2005) showed "multi-target tracking" techniques defeat complete anonymity

Computational Countermeasures: k-Anonymity



I'm chicken # 341, and I'm in this building (along with k-1 other chickens).

I'm chicken # 341, and I visited this place in the past 21 minutes (along with k-1 other chickens).



- k-anonymity introduced for location privacy by Gruteser & Grunwald, 2003
- They note that temporal ambiguity also gives k-anonymity
- Pattern of service requests could break k-anonymity (Bettini, Wang, Jajodia 2005)

Computational Countermeasures: Mix Zones

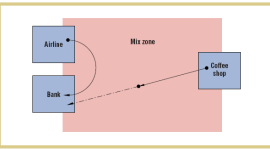
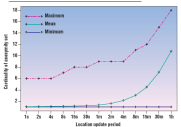


Figure 1. A sample mix zone arrangement with three application zones. The airline agency (A) is much closer to the bank (B) than the coffee shop (C). Users leaving A and C at the same time might be distinguishable on arrival at B.



Beresford & Stajano, 2003

- New, unused pseudonym given when user is between "application zones"
- "k-anonymous" when you can be confused with k-1 other people
- Anonymity (i.e. k) varies with busyness of mix zone
- Attack by trying to list all pseudonyms given to a person
- Can use probabilistic paths to associate pseudonyms

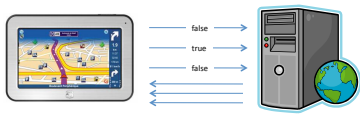
Computational Countermeasures: False Reports

An Anonymous Communication Technique using Dummies for Location-based Services

Hidetoshi Kido¹ Yutaka Yasuyama² Tsunaji Sudo^{1*}
¹ Graduate School of Information Science and Technology, Osaka University
² NTT Communication Science Laboratories, NTT Corporation
 kido@isl.is.tohoku.ac.jp yutaka@isl.is.tohoku.ac.jp sudo@isl.is.tohoku.ac.jp

- Mix true location report with multiple false reports
- Act only on response from true report

Pervasive Services, 2005



- Communication overhead (addressed in paper)
- Attack by finding most sensible sequence of location reports
- Counter by making false sequences sensible (addressed in paper)

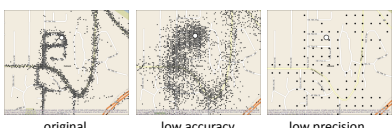
Computational Countermeasures: Obfuscation

A Formal Model of Obfuscation and Negotiation for Location Privacy

Matt Duckham¹ and Lutz Kallh²
¹ Department of Geomatics, University of Melbourne, Victoria, 3010, Australia
 m.duckham@unimelb.edu.au
² Department of Computer Science and Software Engineering, University of Melbourne, Victoria, 3010, Australia
 l.kallh@unimelb.edu.au

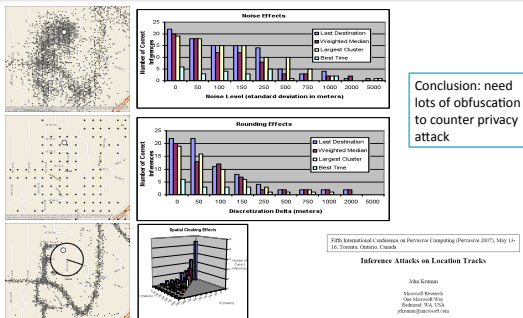
- Formalizes obfuscation techniques
- Client & server can negotiate what needs to be revealed for successful location based service

Pervasive 2005



(from Krumm 2007)

Computational Countermeasures: Obfuscation



Conclusion: need lots of obfuscation to counter privacy attack

©2007 International Conference on Pervasive Computing (Pervasive 2007), May 19-21, Toronto, Ontario, Canada.
Inference Attacks on Location Tracks
 John Krumm
 Microsoft Research
 One Microsoft Way
 Redmond, WA, USA
 jkrumm@microsoft.com

Computational Countermeasures: Obfuscation

Protecting Location Privacy Through Path Confusion

Markus
@MIT, USA
ETS Research
Bergen, The State University of New Jersey
Email: hudson@world.etsu.edu

Mario Greuter
@ETH, CH
ETS Research
Bergen, The State University of New Jersey
Email: greuter@world.etsu.edu

SECURECOMM 2005

Confuse the multi-target tracker by perturbing paths so they cross

Figure 2. Two users move in parallel. The Path Perturbation algorithm perturbs the parallel segment into a crossing segment.

Conclusion

- Why reveal your location?
 - Lots of good reasons
 - Including just to know your own location
- Do people care about location privacy?
 - Not as much as we might expect
- Computational location privacy threats
 - Lots of sophisticated threats
- Location prediction
 - Even possible to infer your future locations
- Computational countermeasures
 - Much work on countermeasures
 - More work necessary as more threats come

© by Thaves
