VLDB 2007

Georgia Institute of Technology COLLEGE of COMPUTING

From Data Privacy to Location Privacy: Models & Algorithms

Ling Liu
Distributed Data Intensive Systems Lab
College of Computing
Georgia Institute of Technology

This is a joint work with Bhuvan Bamba, Bugra Gedik, Peter Pesti, Ting Wang, and partially sponsored by NSF CyberTrust Program. The slides available at www.cc.gatech.edu/~lingliu/tutorials/vldb07tutorial-LingLiu.pdf

Outline

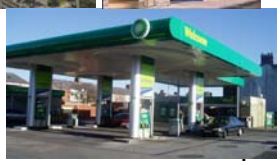
- **Introduction**
  - LBSs and Location Privacy
  - From Data Privacy to Location Privacy
  - Unique Challenges of Location Privacy
- **Location Anonymization Models and Techniques**
  - Alternative Location Privacy Enhanced Service Architectures
  - Location Anonymization Models and Algorithms
    - Trusted third Party Location Anonymization Server model
    - Non-corporative Client-based model
    - Decentralized corporative mobility group model
- **Open Issues and Research Challenges**

Location Based Services (LBSs)

- Resource and information services based on the location of a principal
  - Input: location of a mobile client + information service request
  - Output: deliver location dependent information and service to the client on the move

Location-based Services: Examples

- Location-based emergency services & traffic Monitoring:
  - ***Range query:*** How many cars on the highway 85 north
  - ***Shortest path query***: What is the estimated time of travel to my destination
  - ***Nearest-neighbor query***: Give me the location of 5 nearest Toyota maintenance stores?
- Location-based advertisement/entertainment:
  - ***Range query:*** Send E-coupons to all customers within five miles of my store
  - ***Nearest-neighbor query***: Where are the nearest movie theater to my current location
- Location finder:
  - ***Range query:*** Where are the gas stations within five miles of my location
  - ***Nearest-neighbor query***: Where is nearest movie theater



Location Privacy

- The claim/right of individuals, groups and institutions to determine for themselves, *when, how* and *to what extent* **location information** about them is communicated to others.

- Location privacy also refers to the ability to prevent other parties from learning one's **current or past location.**

Privacy Threats through LBS

- Communication privacy threats
  - Sender anonymity

- Location inference threats [Beresford05, Gruteser&Grunwald03]
  - Precise location tracking
    - *Successive position updates* can be linked together, even if identifiers are removed from location updates
  - Observation identification
    - If *external observation* is available, it can be used to link a position update to an identity
  - Restricted space identification
    - A known *location owned by identity* relationship can link an update to an identity

Privacy Threats: Examples

- Examples
  - Learn about users medical conditions, alternative lifestyles, unpopular political/religious views
  - Spam targeted users with unwanted advertisements
  - Stalking, domestic abuse and physical harms …

[USA Today, Fox News, etc]

http://www.foxnews.com/story/0,2933,131487,00.html

FOX NEWS .com U.S. & WORLD

Updated: 3-28-06 9:42pm ET

SEARCH GO

E-MAIL STORY PRINTER FRIENDLY FOXFAN CENTRAL

Man Accused of Stalking Ex-Girlfriend With GPS

Saturday, September 04, 2004

Associated Press

GLENDALE, Calif. — Police arrested a man they said tracked his ex-girlfriend's whereabouts by attaching a global positioning system (search) to her car.

Ara Gabrielyan, 32, was arrested Aug. 29 on one count of **stalking** (search) and three counts of making criminal threats. He was being held on $500,000 bail and was to be arraigned Wednesday.

"This is what I would consider stalking of the 21st century," police Lt. Jon Perkins said.

Location Privacy: Challenges

- **Challenge 1:**
  - Location Privacy is a personal matter.
  - Different users may have different location privacy requirements.
  - Same users may have different location privacy requirements in different context (time, space).
- **Challenge 2:**
  - Location Privacy v.s. Location Utility
  - On one hand, Location information is useful for enhancing services
  - On the other hand, location information should be disclosed with care to reduce the risk of unauthorized disclosure of users' locations or movement patterns.
- **Challenge 3:**
  - Location Privacy v.s. Location k-anonymity
    - Is location k-anonymity sufficient?

Data Privacy v.s. Location Privacy

Data Privacy

- Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others".

A. Westin. Privacy and Freedom. 1967.

Location Privacy

- Location privacy is the claim/right of individuals, groups and institutions to determine for themselves, when, how and to what extent **location information** about them is communicated to others

Data Privacy: where we are

- Policy-based Privacy Protection
  - Federal Privacy Acts to protect privacy
    - E.g., Privacy Act of 1974 for federal agencies
      - Still many examples of privacy violations even by federal agencies
      - xxx Airways revealed travellers' data to federal gov't
    - E.g., Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Secure Access in Statistical Databases
  - Answering statistical queries without revealing the private (sensitive) data
- Privacy-preserving Data Mining
  - Computing the mining results without access to the raw data

Secure Access in Statistical Databases

- Database contains public information (e.g. zip code) and private information (e.g. income)
  - Client wants to compute statistics on private data of a subset selected by using public data.
  - The database (owner) wants to reveal only the statistical outcome, not private values used for computation.
- **Methods:**
  - Restrict the types of queries allowed to prevent known statistical inference attacks

Privacy-Preserving Data Mining

- Query Independent Data Privacy Protection
  - Privacy-preserving classification
  - Privacy-preserving association rule mining
  - Privacy-preserving clustering
- Databases contain both public information (e.g. zip code) and private information (e.g. income, medical diagnosis)
  - Allow public release of mining results over a data owner's private database, while preventing the disclosure of private (sensitive) information.
  - Allow multiple data holders to collaborate to compute (mine) important statistical (aggregate) information over a collection of private databases, while protecting the privacy of sensitive raw information.
- Methods:
  - K-anonymity and k-anonymization
  - l-diversity, etc.

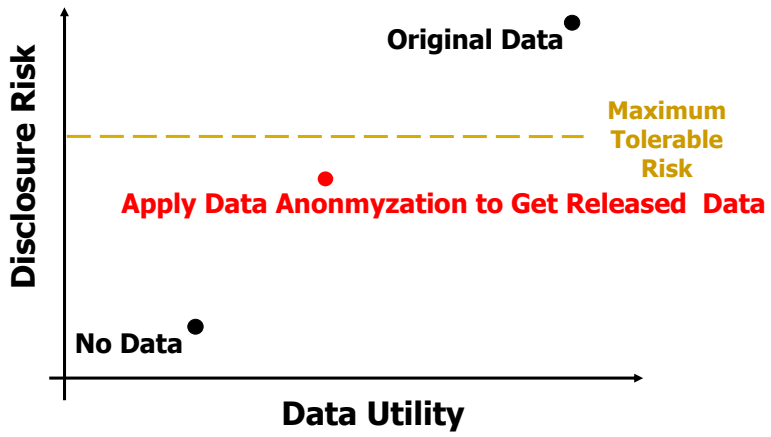
Anonymity Versus k-Anonymity

- Full Anonymity
  - relax the requirement such that the adversary learns nothing about the origin of a given message/query/LBS-request
- k-Anonymity
  - accept k-anonymity, in which the adversary can only narrow down his search (inference) to k participants.
  - Bigger k implies higher degree of obfuscation and higher level of privacy guarantee.

K-Anonymity and K-Anonymization

- Goal: Preserving individual privacy while allowing public release of information
- K-anonymity [Samarati & Sweeney]
  - Each tuple is indistinguishable from at least k-1 others.
- K-anonymization
  - Transform dataset to achieve k-anonymity
  - Optimal transformation
    - in terms of the level of privacy guarantee preserved and the level of data utility obtained

R-U Confidentiality Map



(Duncan, et al. 2001)

k-Anonymity for Relational Tables Limitations and Challenges

- Make sure for each quasi identifier, there are at least *k*-1 other entries with the same set of sensitive data and each associated with a different quasi identifier (pseudo identity) [Sweeny et al.]

	Race	Birth	Gender	ZIP	Problem
t1	Black	1965	m	0214*	short breath
t2	Black	1965	m	0214*	chest pain
t3					
t4	Black	1965	f	0213*	hypertension
t5	Black	1964	f	0213*	obesity
t6	Black	1964	f	0213*	chest pain
t7	White	1964	m	0213*	chest pain
t8	White	1964	m	0213*	obesity
t9	White	1964	m	0213*	short breath
t10	White	1967	m	0213*	chest pain
t11	White	1967	m	0213*	chest pain

Example of *k*-anonymity, where *k*=2 and QI={*Race*, *Birth*, *Gender*, *ZIP*}

Violate l-diversity

1. Identify quasi identifier
2. Remove identifier of each record
3. Ensure k-anonymity of sensitive data columns on quasi-identifier
4. Ensure l-diversity of sensitive data columns

K-Anonymity and K-Anonymization Challenges

- Ensuring *k*-anonymity and *l*-diversity upon transformation [Sweeny] [MachannavajjgalaGehrkeKifer-icde06]
- Ensuring *m*-variance upon updates [ref]
- Optimal k-Anonymity Transformations [SamaratiSweeney] [BayardoAgrawal-ICDE 2005]

Example k-Anonymization Techniques

- Greedy / hill-climbing [Sweeney]
- Stochastic search (simulated annealing [Winkler], genetic algorithms [Iyengar])
- Approximation algorithms [Myerson & Williams] [Aggarwal et al]
- Generalization/Supression [SamaratiSweeney]
- Top-down specialization [Bertinoetal+ICDE'05, Fung+CDE'05]
- Optimal Bucketization [HoreMehrotraTsudik-vldb]
- Optimal k-Anonymization [Roberto J. Bayardo Rakesh Agrawal ICDE 2005]

Location Privacy Protection

- Prevent disclosure of unnecessary information (the individual identity and location of an individual) through explicitly or implicitly control of what information is given to whom and when.

- Challenges
  - Disclosure through direct communication
  - Disclosure through observation
  - Location Privacy Exposure through inference of location combined with other properties of an individual
    - such as interests, behavior, or communication patterns could lead to the identity and location by inference or statistical analysis.

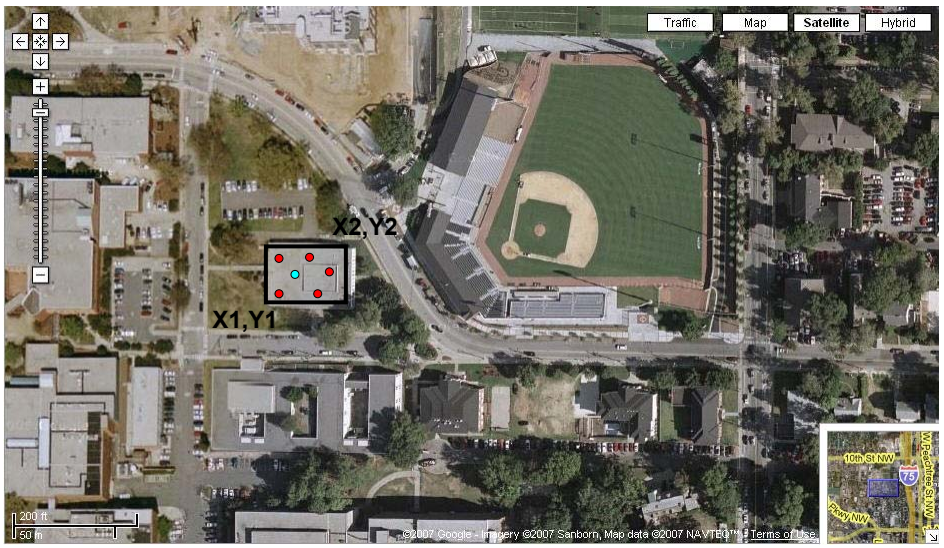
Location Anonymity

- **Location Anonymity**
  - The system property that guarantees that the inability to associate location information to a particular individual/group/institution through inference attacks.
- **Location k-anonymity** k or more users at the same location
  - Make sure for each location query message, there are at least ***k-1 other messages (entries)*** with the same location information, each associated with a different (pseudo) identity
  - It guarantees that the adversary can only associate location information to ***k*** participants instead of to a particular individual/group/institution through inference attacks
- **Location l-diversity** *l* or more still objects at the same location
  - For each location query message, in addition to user level k-anonymity (k different user identities), there are at least ***l* different still location objects** associated with each of the k users.

Location k-Anonymization

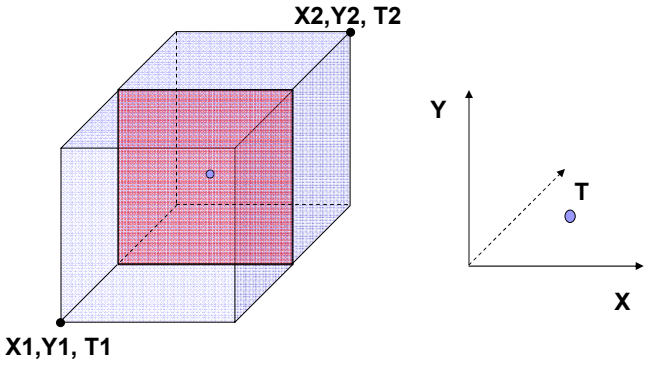
- Main ideas
  - Applications can tolerate *inaccurate location data* to a certain degree
  - Location perturbation provides the inability for adversaries to know or infer exact location of a user through location based inference (k>1)
- Approaches:
  - Spatial Cloaking
  - Spatio-temporal Cloaking
  - Geometric Transformation

Spatial Cloaking



Spatio-Temporal Cloaking

Spatial Cloaking First and followed by Temporal Cloaking



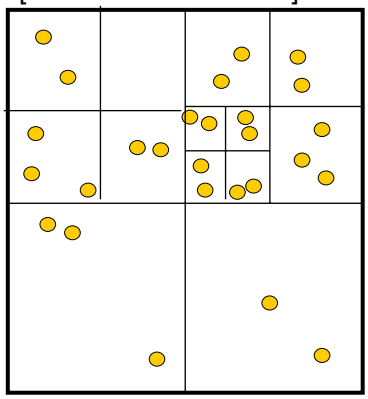
Challenge 1: Location Privacy and Personalization

- Guideline1: User Choice (policy based)
  - Location privacy issues can be placed into three categories depending on the user choice (consent) in the use of the technology that is tracking location:
    - **Active use**: the individual is a willing participant
    - **Passive use**: information used without the individual's knowledge or permission
    - **Flexible use**: covers devices whose use has the unintended consequence of tracking location information.
- Guideline 2: Personalized Location Perturbation

Universal Location *k*-Anonymity

- Randomly replace identifiers to prevent tracking
- Anonymize by replacing point location information in each message with a spatial cloaking box
- For each message, make sure that there are at least *k*-1 other messages from different mobile units, with the same cloaking box
- Extend 2D spatial cloaking to 3D spatio-temporal cloaking
  - **spatial obfuscation by 2D k-anonymization box**
  - **Temporal obfuscation by delaying messages-3D k-anonymization box**

[Gruteser&Grunwald03]



Problems with Universal k-Anonymity

- A system-wide static *k* value
- Not possible to support
  - users with different privacy requirements,
  - different privacy requirements of a user at different times
- No QoS guarantees
  - No upper limit on the size of the spatiotemporal cloaking box, meaning
    - no guarantees on maximum tolerable spatial resolution
    - no guarantees on maximum tolerable delay
- Not possible to dynamically make privacy/QoS and privacy/performance tradeoffs on per message and per user basis

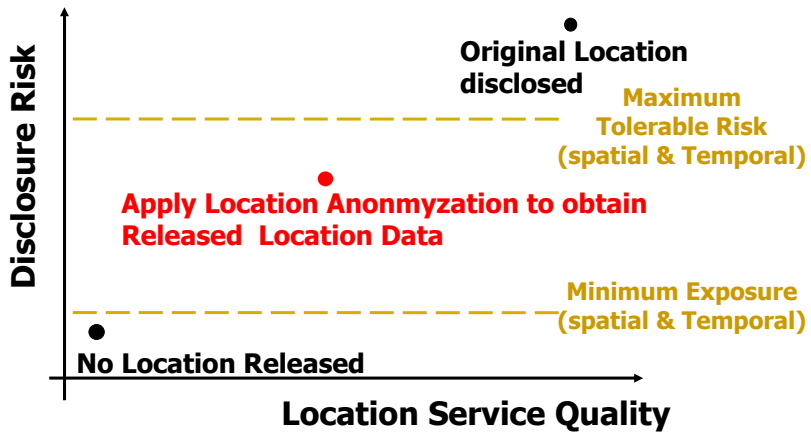
Personalized Location Anonymity

- Advocate personalized k-anonymity (l-divisity) instead of a system-wide universal *k* (or l) value
  - Enable different users to define different privacy requirements
  - Enable a user to have different privacy requirements at different times and in different contexts
- Support QoS guarantees
  - setting user and application specific upper bound on the size of the spatio-temporal cloaking box
    - upper bound on spatial resolution within an acceptable scope
    - upper bound on temporal resolution to constrain the delay within acceptable range
- Allowing dynamically making privacy/QoS and privacy/performance tradeoffs on per message and per user basis

Challenge 2: Location privacy v.s. Location Service Quality

- Quality (Utility) of Services
  - Applications can tolerate inaccurate location data to a certain degree (e.g., E-911)
- Can we "hide" data to protect privacy while providing desirable utility of the location data and LBSs?
  - Ambiguous location information may lead to certain degradation in the quality of the service
  - Trade off between quality of services and degree of location privacy
- Technical Challenge
  - How to balance location privacy and service quality?

Challenge 2: Location Privacy and LBS Quality Tradeoffs



[GedikLiu-ICDCS 2005, TMC 2007]

Location Anonymization Profile

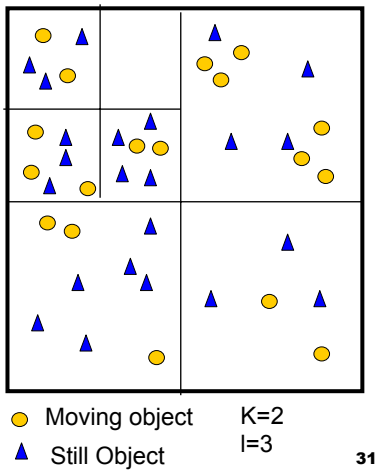
- Per User or Per message based
- Five basic components
  - K-anonymity w.r.t. users
  - L-diversity w.r.t. still objects (publicly known landmarks and locations)
  - Minimum spatial resolution willing to be disclosed
  - Maximum tolerable spatial resolution
  - Maximum tolerable temporal resolution

Personalized location anonymization constraints

Personalized location service quality constraints

Challenge 3: Location Anonymization by k-anonymity and l-diversity

- Stronger location privacy guarantee by carefully combining k-anonymity and l-diversity
- Location anonymization is measured by f(k, l) → location disclosure risk is 1/(k*l) < 1/k.



Key Factors in Location Privacy

- Location Anonymization Challenges
  - Personalized Location Privacy
  - Tradeoff between location privacy and service quality
  - Strong and Weak Location Anonymization
- Location Types
  - Public v.s. Private
- Location Privacy Threat Models
  - Determines the type of service architecture(s) for location privacy protection

Different Types of Location Data

- Geometric v.s. Symbolic location models
- Public v.s. Private Location
  - Public Location Data:
    - All still objects that are accessible or visible from roads are publicly known locations.
    - Postal addresses available in yellow-book, white-book, Google Earth
  - Private Location Data
    - Location updates of a mobile client
    - Movement patterns of mobile clients

Factors Affecting Location Privacy

- Location Privacy Protects
  - Private location data
  - The linkage of private location data with public locations
- Three types of LBSs
  - LBSs that require true identity
    - Security policy, Cryotography techniques
  - LBSs that require only pseudonyms
    - Privacy policy, Pseudonym maintenance protocols, location anonymization
  - LBSs that does not require pseudonyms
    - Privacy policy, location anonymization

Part II
Location Anonymization
Models & Techniques

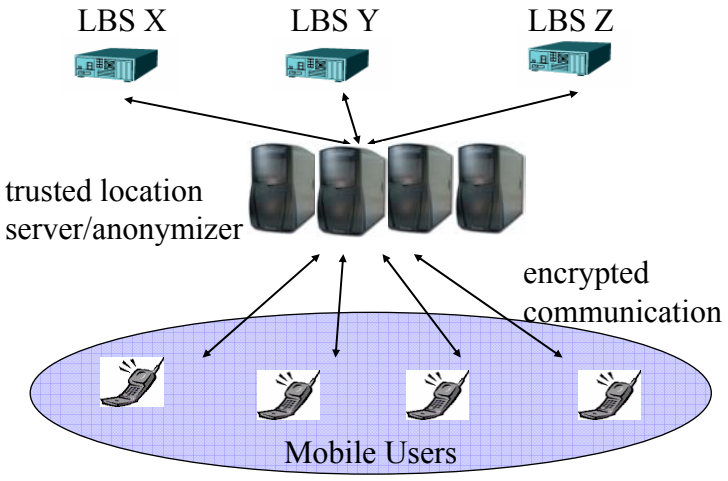
Location Anonymization Models:

- Centralized Trusted third party Location Anonymization Model
  - A trusted third party anonymization proxy server is served for both location updates and location anonymization.
  - Capable of supporting customizable/personalized location k-anonymization
- Client-based non-cooperative Location Anonymization Model
  - Mobile clients maintain their location privacy based on their knowledge
  - Location cloaking without location k-anonymity support
- Decentralized corporative mobility group model
  - A Group of mobile clients collaborate with one another to provide location privacy of a single user without involving a centralized trusted authority.
- Distributed Hybrid Architecture with limited cooperation

Trusted Third Party Location Anonymization Model

- Require a third party anonymization proxy (middleware) for all communications between mobile users and LBS applications
- Through the location proxy, LBS applications receive and reply to anonymous messages from the users
  - Mobile clients
    - use dedicated location severs to track their location updates and relay their location service requests to appropriate LBSs.
  - LBS applications
    - register with the mobile clients' location servers
    - Request for Event call backs for possible containment in spatial region being tracked

Centralized Trusted Third Party System Architecture



Location Privacy Threat Model

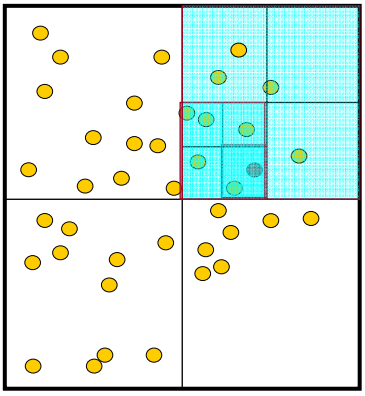
- Most commonly used location privacy threat model
  - Hide the true identity of mobile users from LBSs → security policy
  - Considering LBSs that accept pseudonyms
  - Regarding LBS applications as hostile observer
    - Setting constraints on what information can and cannot be revealed from one LBS to another may not be sufficient
  - But trust the location sensing infrastructure and location server/location anonymizer
    - raw location acquisition systems, such as GPS, WiFi, and several indoor locators (e.g., Cricket)
    - Location servers/anonymizers – handling location updates and location anonymization

Location Perturbation Techniques

- Spatio-temporal cloaking
  - Quadtree-based approach [GrusteserGrunwald03]
  - Graph Clique based approach [GedikLiu05]
  - Casper pyramid-based approach [MokbelChowAref06]
  - PrivacyGrid [BambaLiu07]
  - Geometric Transformation
    - Distance preserving for range and kNN queries
    - Inference Attack Resilient Geometric Transformations [ChenLiu2005, ChenLiu2007]

Quadtree Spatial Cloaking

- Recursively divide the space into quadrants until a quadrant has less than *k* users.
- The previous quadrant, which still meet the *k-anonymity* constraint, is returned
- Pros:
  - Achieve location *k-anonymity*, i.e., a user is indistinguishable from *k-1* other users
- Cons: Universal k
  - no support for personalized location privacy

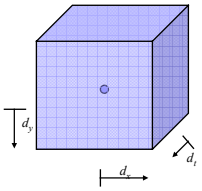


Achieve k-anonmity with k=4

ClickCloak Algorithms: Peronalized Location k-Anonymization

- Introduce a personalized *k*-anonymity model. Each message can specify:
  - a different *k* value based on its specific privacy requirement
  - Maximum spatial and temporal (resolution) tolerance values based on its QoS requirements
- The location cloaking algorithm *CliqueCloak* is capable of
  - supporting customizable location *k*-anonymity model
  - continuously processing a stream of messages

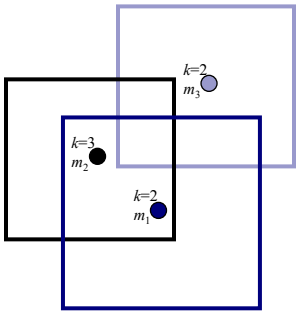
Message Anonymization



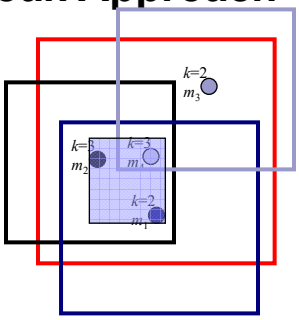
- Two sets of messages
  The raw message set S:
  - $m_s \in S$:⟨u_{id}, r_{no}, {x, y, t}, k, {d_x, d_y, d_t}, C⟩
    - $P(m_s) = (x, y, t)$, ***spatio-temporal point***
    - $B_{cn}(m_s) = (\Phi(m_s.x, m_s.d_x), \Phi(m_s.y, m_s.d_y), \Phi(m_s.t, m_s.d_t))$ ***spatio-temporal constraint box,*** $\Phi(v, d) = [v-d, v+d]$

  The transformed (anonymized) message set T:
  - $m_t \in T$:⟨u_{id}, r_{no}, {X:[x_s, x_e], Y:[y_s, y_e], I:[t_s, t_e]}, C⟩
    - $B_{cl}(m_t) = (X, Y, I)$, ***spatio-temporal cloaking box***
- For each message in S, there is at most one anonymized message in T
  - $m_t = R(m_s)$, where $(m_s.u_{id}, m_s.r_{no}) = (m_t.u_{id}, m_t.r_{no})$
- u_{id}, r_{no} fields are removed from the messages in T, and are replaced by a random dummy identifier before the messages can be exported to LBS providers

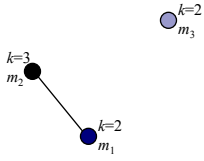
Illustration of ClickCloak Approach



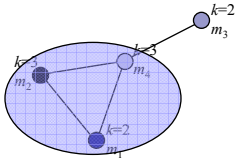
spatial layout I



spatial layout II

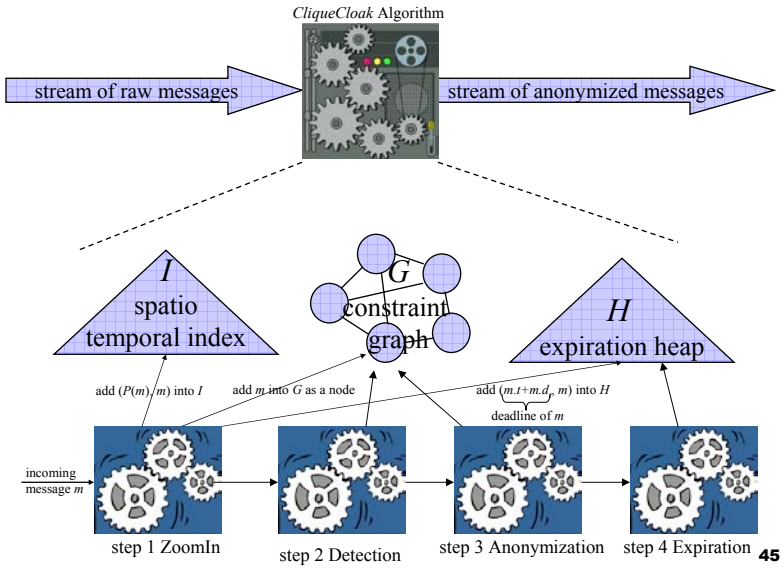


constraint graph I



constraint graph I

Location Cloaking - CliqueCloak



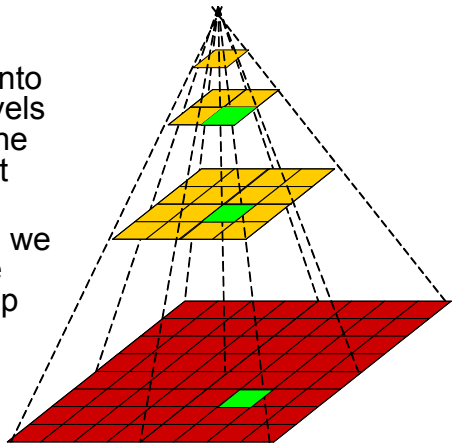
Customized Location Anonymization Model

- A unified framework for personalized k
  - handling personalized and customizable privacy requirements through k-anonymization with variable k
- QoS guarantees by ensuring
  - spatial cloaking box meets users' maximum spatial (spatio-temporal) resolution (tolerance)
  - spatio-temporal box meets user's maximum tolerable delay (max temporal resolution)
- Intelligent tradeoff
  - between privacy and utility of location data

Casper Approach

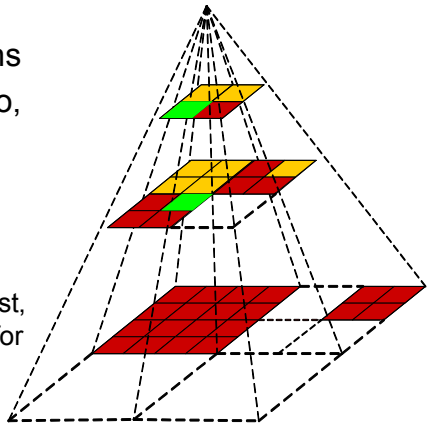
[MokbelChowAref+vldb06,Mokbel-MDM 2007]

- The universe of discourse is represented as a *complete pyramid* structure
- The basic pyramid is divided into grids at different resolution levels and each grid cell maintains the number of mobile users in that cell
- To anonymize a user request, we traverse the pyramid structure from the bottom level to the top level until a cell satisfying the user privacy profile is found.
- Pros: Simple to implement.
- Cons: Overhead in finding cloaked region and in maintaining all grid cells



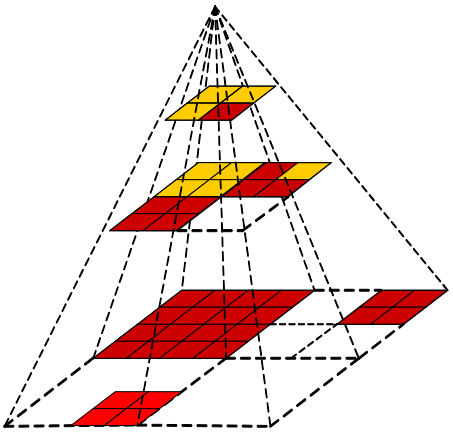
Casper: Adaptive Pyramid Structure

- Instead of maintaining all pyramid cells, only maintain those cells that are potential cloaked regions
- Similar to the basic pyramid algo, traverse the pyramid structure from the bottom level to the top level, until a cell satisfying the user privacy profile is found.
- Pros: Find the cloaked region very fast, most of the time in only one hit, good for fix k per user
- Cons: Overhead in maintaining adaptive pyramid, bad for variabke k per message



Casper: Adaptive Pyramid Maintenance

- The adaptive pyramid structure dynamically adjusts its maintained cells based on users' mobility.
- *Cell Splitting:* Whenever a user in a certain cell expresses relaxed privacy profile (reduce k value), the cell is split into four lower cells.
- *Cell Merging:* only when all users within certain cells strength their privacy profiles (increase k value), those cells can be merged together



PrivacyGrid

[BhuvanBambaLingLiu-2007]

Location Anonymization Server

- CliqueCloak location cloaking
  - Model location messages among users of a particular LBS in a constraint graph
  - Finding a clique in the graph
  - Pros: small cloaking box
  - Cons: not scalable, only efficient for small k (k < 10)
- Pyramid Cloaking
  - Non-optimal anonymization → low success rate
  - Bad for per-message based k-anonymization
- PrivacyGrid cloaking (LP Enhanced Grid Index based location cloaking)
  - Optimal anonymization → high success rate with larger k
  - Highly efficient for both per user and per message based location anonymization

Location Perturbation Requirements

- A unified framework
  - for handling personalized and customizable privacy requirements through k-anonymization.
- QoS guarantees by ensuring
  - spatial (spatio-temporal) cloaking box meets users' maximum spatial (spatio-temporal) resolution (tolerance).
- Intelligent tradeoff
  - between privacy and utility of location data
- **Enhanced location anonymization semantics**
  - **Location k-anonymity**
  - **Location l-diversity**
- **Fast cloaking algorithm**
  - keeping perceived delays as low as possible.
- **Efficient techniques for processing location cloaked queries**
  - Extensions to existing query processing methods

PrivacyGrid: Basic Framework

- User Privacy Profile
  - Original message:

    $\{ u_{id}, m_{id}, \{ x, y \}, k, l, \{ d_x, d_y, d_t \}, F \}$

- u_{id}, m_{id} fields in the original messages are replaced by a dummy identifier before forwarding the messages to a LBS.

- Location P3P:
  - $\{k, l, \{d_x, d_y, d_t\}\}$ are parameters for supporting user desired privacy preferences in terms of location privacy measure and location service quality measure
  - Location k-anonymity - ***k***
  - Location l-diversity - ***l***
  - Location Service Quality
    - Maximum spatial resolution - (d_x, d_y)
    - Maximum temporal resolution - d_t

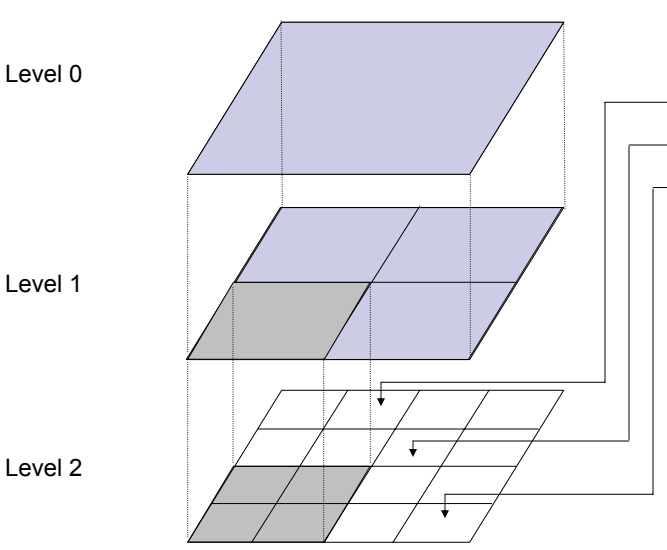
Location Anonymization Server

- **A cluster of location servers**
  - Handling location updates and location query perturbations

- Location Perturbation
  - Cloak messages among users of a particular LBS and forward cloaked anonymous queries or updates to the respective LBS.

- Spatio-temporal Cloaking algorithms
  - Grid Index based Algorithms

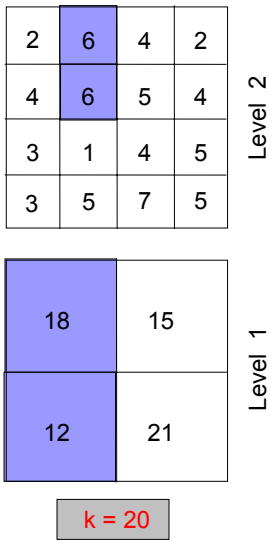
Hierarchical Quad Grid Index



OBJECT ID	CELL ID
1	
2	
3	
……	
……	
……	
9998	
9999	
10000	

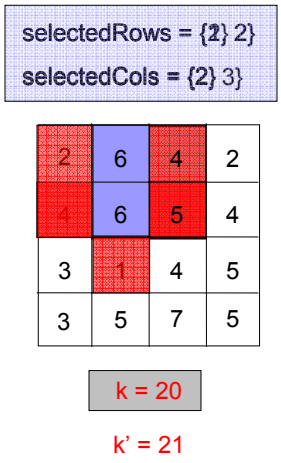
Basic Grid-Based Cloaking

- Quad Grid Cloaking
  - Assume a grid of cells over the entire geographical area of interest.
  - A location query is posed by a mobile user residing in a grid cell C_i.
  - Test k-anonymity for cell C_i and if it contains k moving objects, chose C_i as the optimal cloaking region,
  - If C_i contains less than k moving objects, expanding the cell using horizontal or vertical cells of the base cell C_i,
  - If not enough, expand to the next level grid cell
  - Repeat the steps 3 and 4 until the smallest cloaking box is found
- Pros
  - Very Fast in finding a cloaking box
  - Highly efficient for both per-user and per-message based location anonymization
- Cons
  - Anonymitzation is not optimal (the cloaked box computed may be oversized and too big than necessary) Due to the fact that the cloaked area expands very rapidly.
  - Low anonymization success rate



Bottom-Up Grid Cloaking

- Key Steps
  - Starts with grid cell containing object whose location needs to be cloaked.
  - Selects rows or columns to add in each iteration.
  - Until k-anonymity provided by selected rows/columns meets required levels.
  - Return cells covered by selected rows/columns.
- Pros
  - Attempts to meet optimal anonymity values (k and l)
  - Slowly expand by adding new cells to cloaked region.
  - High success anonymization rate
- Cons
  - Slower than the Quad Grid cloaking.



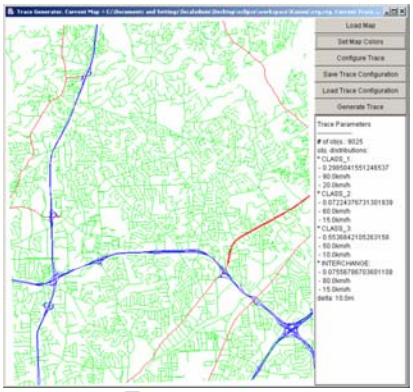
Grid-Based Cloaking: a Summary

- Grid-based Cloaking Algorithms
  - Basic Quad Grid Cloaking
    - Fast but constrained by quad grid expansion thus low success rate of anonymizaton
  - Dynamic Bottom-Up Grid Cloaking
    - Expanding grid cells from bottom up to find the optimal cloaking box for each location query
  - Dynamic Top-Down Grid Cloaking
    - Expanding grid cells from top down from the maximum spatial resolution specified by the user location P3P and to find the optimal cloaking box for each location query
  - Hybrid Dynamic Grid-based Cloaking
    - Exploit different ways of combining bottom up and top down.

Top-Down Grid Cloaking

- Key Steps
  - Starts with maximum cloaking area allowed by spatial tolerance values.
  - Selects rows or columns to remove in each iteration.
  - Until k-anonymity provided by selected rows/columns falls below required levels.
  - Return selected rows/columns from previous iteration.
- Pros
  - Attempts to meet optimal anonymity values.
  - Higher anonymization success rate
- Cons
  - Slower than quad grid cloaking.

Experimental Setup



Trace generator

mean of car speeds for each road type	$\{90, 60, 50\} km/h$
std.dev. in car speeds for each road type	$\{20, 15, 10\} km/h$
traffic volume data	$\{2916.6, 916.6, 250\}$per hour

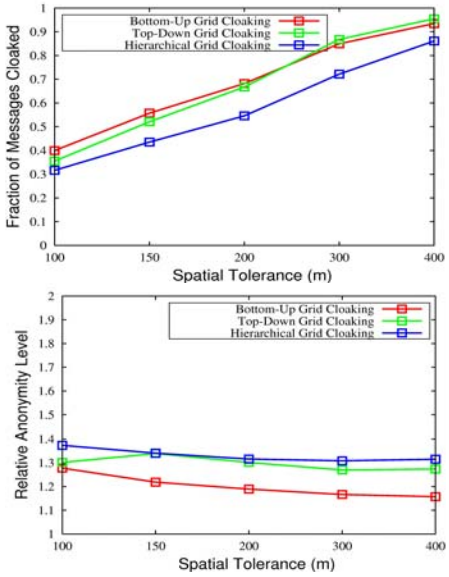
Car movement parameters

- Road data available from United States Geological Survey (USGS) in SDTS format
- Use transportation layer of 1:24K Digital Line Graphs (DLGs)
- Extract three types of roads
  - class 1 (expressway)
  - class 2 (arterial)
  - class 3 (collector)
- Map from Chamblee region of Atlanta, Georgia
- Covers a region of ≈ 160 km^2
- Use real traffic volume data to calculate the number of cars on each road type
- Each car generates several messages during the simulation.
- The maximum spatial and temporal resolution values of the messages are selected independently using normal distributions

Evaluation Metrics

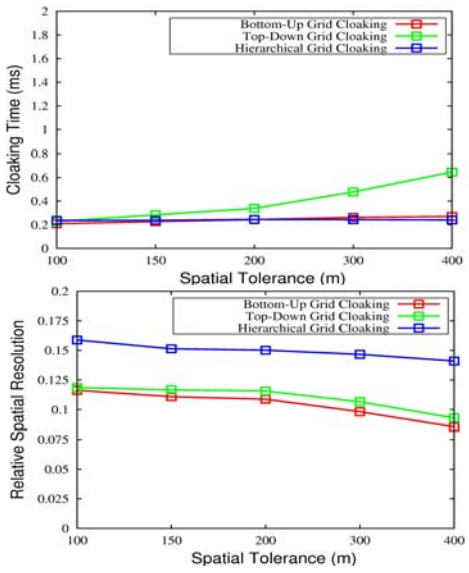
- *Success Rate*:
  - 100*|*T*|/|*S*|
- *Relative Anonymity Level*:
  - $\frac{1}{T} \sum_{m_s = R(m_s) \in T} \frac{\left|\{m : m \in T \wedge B_{cl}(m_t) = B_{cl}(m)\}\right|}{m_s.k}$
- *Relative Temporal Resolution*:
  - $\frac{1}{T} \sum_{m_t = R(m_s) \in T} \frac{2 * m_s.d_t}{||m_t.I||}$
- *Relative Spatial Resolution*:
  - $\frac{1}{T} \sum_{m_t = R(m_s) \in T} \sqrt{\frac{2 * m_s.d_x * 2 * m_s.d_y}{||m_t.X|| * ||m_t.Y||}}$
- *Message Processing Time*:
  - Time to process 10^3 messages

Experiment 1: Grid-based Cloaking



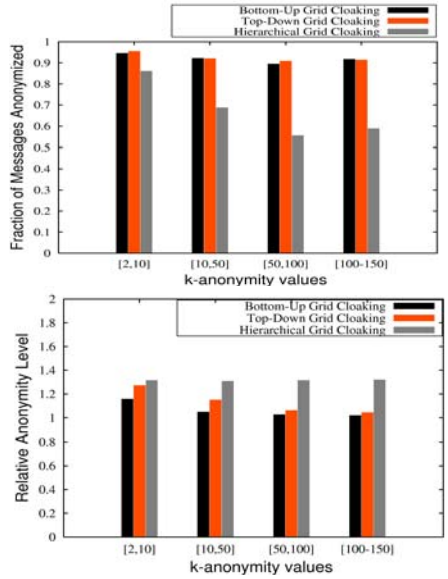
- *K-anonymity values* between 2 and 150, following Zipfian distribution with zipf value 0.6
- Bottom-Up and Top-Down Grid Cloaking algorithms are able to successfully anonymize higher number of messages at same spatial tolerance values.
- Bottom-Up Grid Cloaking provides better relative anonymity values.

Experiment 2: Grid-based Cloaking



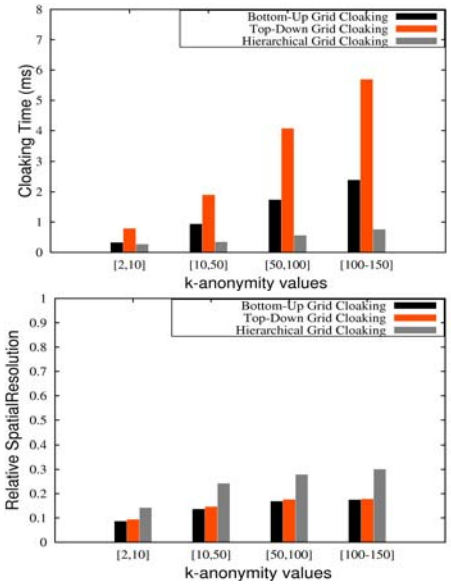
- Bottom-Up Grid Cloaking and Hierarchical Grid Cloaking are faster.
- Relative Spatial Resolution is lower for the Bottom-Up and Top-Down Grid Cloaking algorithms (better QoS).

Experiment 3 Grid-based Cloaking



- Higher *k-anonymity values (*up to k = 150*).*
- Bottom-Up and Top-Down Grid Cloaking algorithms are able to successfully anonymize higher number of messages.
- Bottom-Up and Top-Down Grid Cloaking algorithms provide better relative anonymity values.

Experiment 4 Grid-based Cloaking

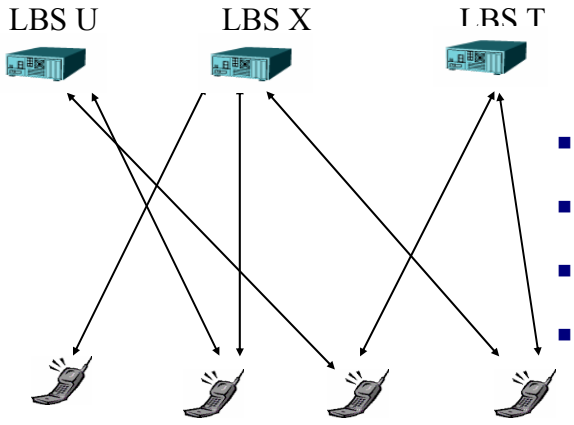


- Hierarchical Grid Cloaking algorithm is extremely fast. All algorithms take a few milliseconds.
- Bottom-Up and Top-Down Grid Cloaking provide better spatial resolution.

Location Anonymization Models:

- Centralized Trusted third party Location Anonymization Model
  - A trusted third party anonymization proxy server is served for both location updates and location anonymization.
  - Capable of supporting customizable/personalized location k-anonymization
- **Client-based non-cooperative Location Anonymization Model**
  - Mobile clients maintain their location privacy based on their knowledge
  - Location cloaking without location k-anonymity support
- Decentralized corporative mobility group model
  - A Group of mobile clients collaborate with one another to provide location privacy of a single user without involving a centralized trusted authority.
- Distributed Hybrid Architecture with limited cooperation

Client-based non-cooperative Location Anonymization Model



- Location obfuscation performed at client
- Location Query with cloaked location
- Encrypted communication
- Exact answer to be filtered at the client

Location Privacy Threat Model

- Hide the true identity of mobile users from LBSs → security policy
- Considering LBSs that accept pseudonyms
- Regarding both LBS applications and location anonymizers as hostile observer
- But trust the location sensing infrastructure and location anonymizer resided on mobile client
  - raw location acquisition systems, such as GPS, WiFi, and several indoor locators (e.g., Cricket)
  - Client based location anonymizer – only send out anonymized location updates and location queries

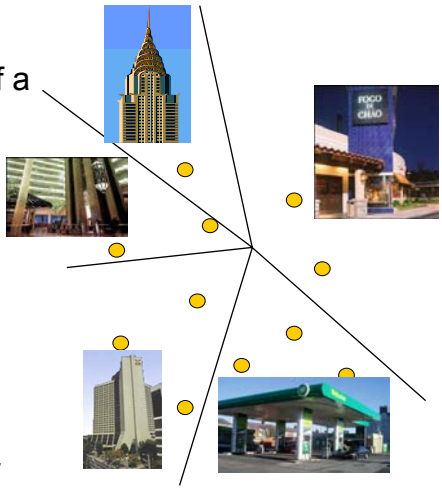
Client-based Location Obfuscation Techniques

- Goal: hide the client identity and the exact location of the client by providing pseudonomity and uncertainty to its location information.

- Example techniques [Roussopoulos et.al USITS99, iPDA-XuDuTangHu 07]
  - Using either the nearest landmark or k-nearest Landmarks instead of the client's current location.
  - Spatial cloaking of the exact location with a coarse spatial region, which includes k-1 other locations such that the client may visit with nearly equal probability, such as k buildings in Georgia Tech campus, k-different stores in lenox sequare.
  - Using the Personal Proxy to route, preserve location privacy, and enable receiver control.

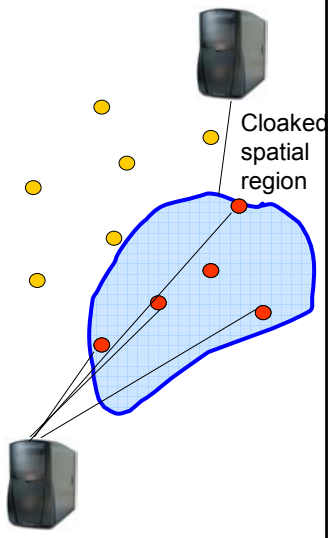
Landmark-based Approach

- Instead of reporting the exact location, report the location of a closest landmark
- Using Voronoi diagrams to identify the closest landmark
- The query answer will be based on the landmark
- Example:
  - Asking near by gas stations will be transformed to
    - Locating the nearest landmark object
    - Return the gas stations near by the landmark object instead of near by the current location of the mobile client



Non-cooperative Architecture: Location Obfuscation

- **Consider a set of locations of the clients within certain spatial vicinity**
- **A client obfuscate her exact location by an enlarged spatial region covering multiple location points (e.g., I am within GT campus or the piedmont park)**
- **The exact location is abstracted as**
  - **either a set of client's past/future location points**
  - **or an enlarged spatial bounding box by location obfuscation at the client**
- **The LBS server evaluates**
  - **the queries based on the distance to each location point or**
  - **evaluate the cloaked location query**
  - **Client filers the answer to its actual query**

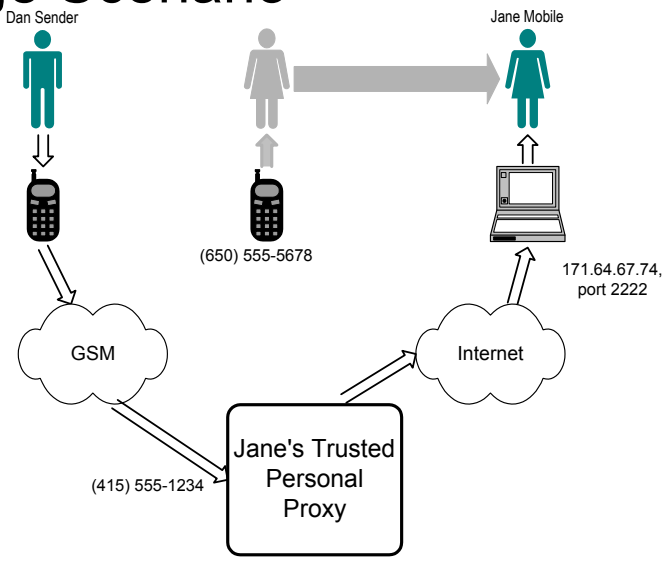


Personal Proxy Approach

[Roussopoulos et.al USITS99]

- Add an extra-level indirection: the Personal Proxy
- You trust your Proxy to preserve your location privacy

Usage Scenario



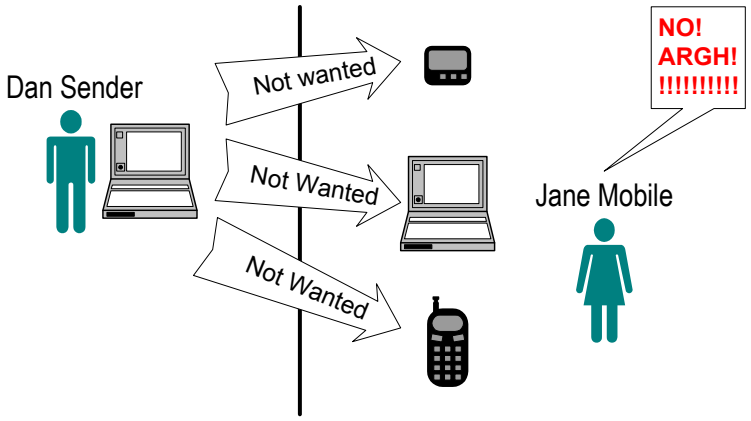
[Roussopoulos et.al USITS99]

Problem: Thwarting Spam

- Continuous reachability could propagate spam!

[Roussopoulos et.al USITS99]

Example:
Spam Goes where Jane Goes



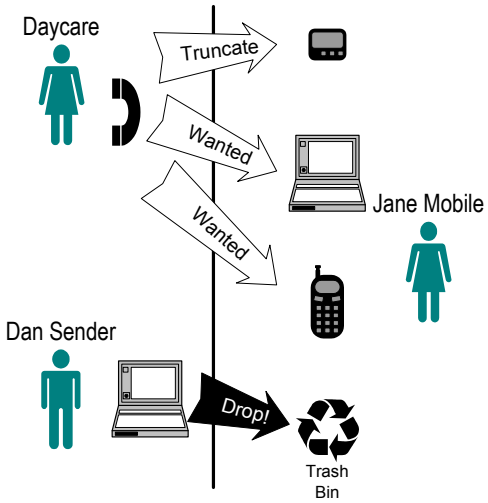
[Roussopoulos et.al USITS99]

Solution: Incorporating location privacy policy

- Personal Proxy filters communication according to user preferences.
- People should be able to control how, when, and where they receive communication.

[Roussopoulos et.al USITS99]

Example: Jane wants control



[Roussopoulos et.al USITS99]

Location Anonymization Models:

- Centralized Trusted third party Location Anonymization Model
  - A trusted third party anonymization proxy server is served for both location updates and location anonymization.
  - Capable of supporting customizable/personalized location k-anonymization
- Client-based non-cooperative Location Anonymization Model
  - Mobile clients maintain their location privacy based on their knowledge
  - Location cloaking without location k-anonymity support
- **Decentralized corporative mobility group model**
  - A Group of mobile clients collaborate with one another to provide location privacy of a single user without involving a centralized trusted authority.
- Distributed Hybrid Architecture with limited cooperation

Peer-to-Peer Cooperative Architecture

- Mobile users form a cooperative network to support their customized location privacy
- Built on top of mobile peer-to-peer communication technologies
- Pros: No need for a third trusted party
- Cons: support weak location privacy
- *Examples:* Group Formation and PRIVE

Location Privacy Threat Model

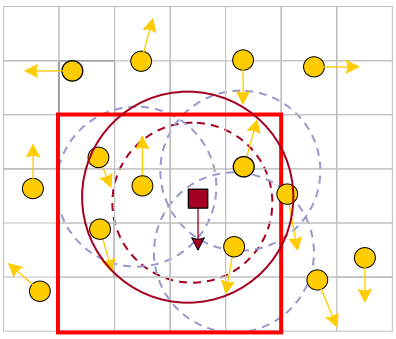
- Hide the true identity of mobile users from LBSs → security policy
- Considering LBSs that accept pseudonyms
- Regarding both LBS applications and location anonymizers as hostile observer
- But trust
  - the location sensing infrastructure and location anonymizer resided on mobile client
  - Peers within the mobility group

Peer Group Formation [Ghinita+www07]

- **Main Idea**
  - Whenever a user wants to issue a location-based query, the user broadcasts a group formation request to its neighbors.
  - Based on the response the user forms an location anonymos group and a member of the group is randomly selected to act as the query sender.
- ***On-demand mode***
  - A mobile user only forms an anonymous group when it needs it.
- ***Proactive mode***
  - Mobile users periodically execute the on-demand approach to maintain their anonymous groups

Group Formation [Ghinita+www07, Mokbel MDM07]

- **Phase 1: Peer Searching**
  - Broadcast a multi-hop request until at least *k*-1 peers are found
- **Phase 2: Location Adjustment**
  - Adjust the locations using velocity
- **Phase 3: Spatial Cloaking**
  - Cloak user location into a region aligned to a grid that cover the *k*-1 nearest peers

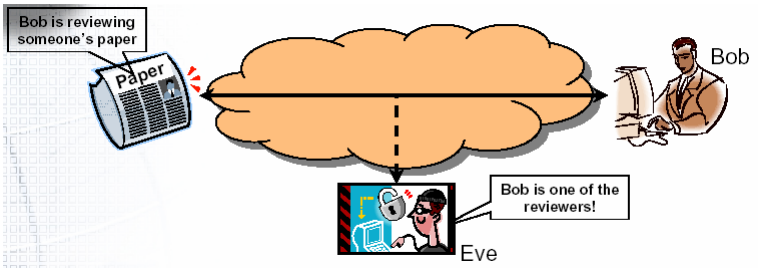


Example: $k = 5$

Location Anonymization: Summary

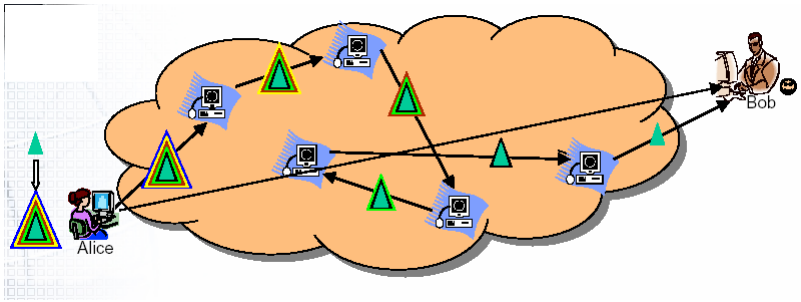
- Using location hiding techniques to disable adversaries to associate *location-based service requests and location updates* with a particular individual
- Representative techniques
  - Location Anonymization through Spatial Cloaking (Data/Information/Messaging Layer) [Gedik&Liu05,Gruteser&Grunwald03, MokbelChowAref2006, BambaLiu07]
  - Anonymous Routing (network layer) [GoldschlagReed99-OrionRouting,KongHong2003-ANODR]
    - Chaum MIXes in Mobile Communication Systems [Chaum81, Federrath et.al96]
  - Mix Zones [Beresford 2003]
  - Location Query Perturbation (Query/Application Layer)

Anonymous Communication



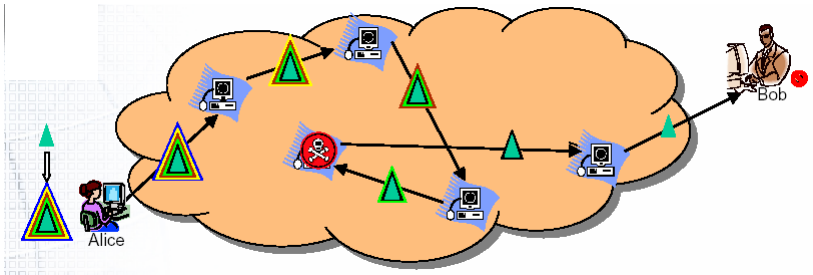
- Bob and the Server want to prevent outsiders from knowing the fact that they are communicating
  - Unlinkablility
- Bob wants to prevent the server from knowing its identity
  - Sender (Source) anonymity

Chaum-Mix



- Standard model for anonymous routing
- Forward messages through a static path of standard nodes P_1 … P_L.
- Encrypt message M using public node keys in reverse order.

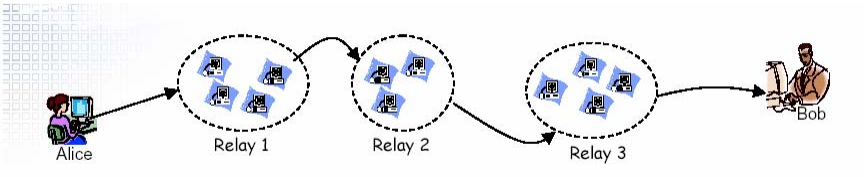
Chaum-Mix



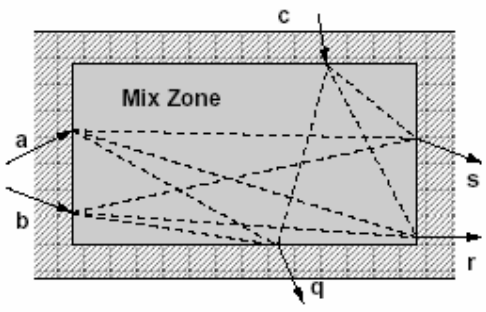
- Drawback: path is fragile and hard to maintain
  - When any link/node fails, must rebuild entire path (expensive)
  - Source cannot receive error messages, must use E2E time out.
- Drawback:
  - Computationally expensive
  - Each message is encrypted with layers of asymmetric encryptions

Anonymous Routing [Zhuang et.al, NSDI 05]

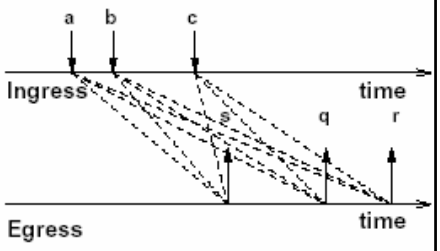
- Cashmere Design
- Using groups to relay traffic
- Relay function if at least one member is reachable



Mix Zones [Beresford et.al]



Plan view of the mix zone



Timeline of movements

Part III Open Issues

Summary

- *Personalized k-anonymity* is a promising approach towards solving the location privacy problem.
- Spatio-temporal cloaking is an efficient framework for providing personalized location k-anonymity
- Among algorithms discussed, Grid cloaking algorithms are fast, efficient and meet diverse users' privacy and QoS specifications.

- Open Issues and Ongoing work
  - Other data privacy techniques
    - Space transformation by rotations
  - Other Location Privacy Protection techniques that do not rely on third party trusted location anonymizer
    - Such as client solutions, user-GUI assisted solutions, decentralized approach
  - Integrating with location security solutions
    - Countering Location transmission threats
    - Secure location claims

Open Issue (1): Enhancing Existing Location Anonymization Techniques

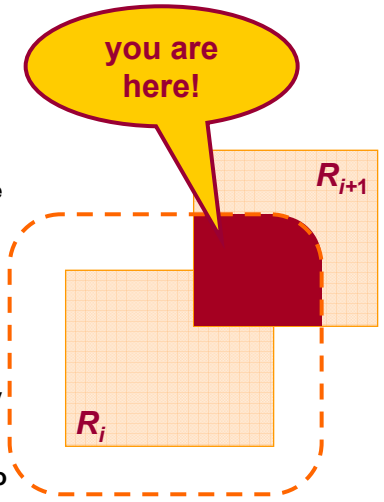
- Extending other data privacy techniques to location anonymizationExample: Space transformation by rotations
- Alternative Client-based or Decentralized techniques that do not rely on trusted third party location anonymizer
  - Example: user-GUI assisted solutions, decentralized approach with stronger privacy guarantee
- Integrating with location security solutions
  - Countering Location transmission threats
  - Secure location claims

Open Issue (2): Potential Attacks to location anonymization solutions

- Understanding different attacks
  - Mobility Model based Attacks
  - Overlaping Spatial/Temporal Window based attacks
- Developing attack resilient solutions

Mobility Model based Attack

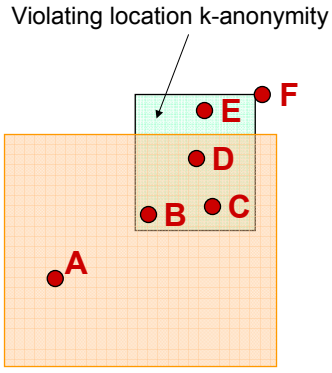
- **Attack utilizing knowledge about motion parameters such as maximum velocity, known Trajectory, frequent travel path**
- **Example 1: Maximum velocity based attack**
- **Adversary can link location with the identifier by obtaining consecutive cloaked location update/query boxes that are overlapping with one another, a**ssuming
  - the same pseudonym is used for two consecutive updates continuous location updates/queries
  - The maximum possible speed is known
- **The maximum speed can be used to compute the maximum movement boundary of the same pseudonym**
- **The user is located at the intersection of two cloaked spatial regions**



[Mokbel MDM07]

Overlapping Window based Inference Attack

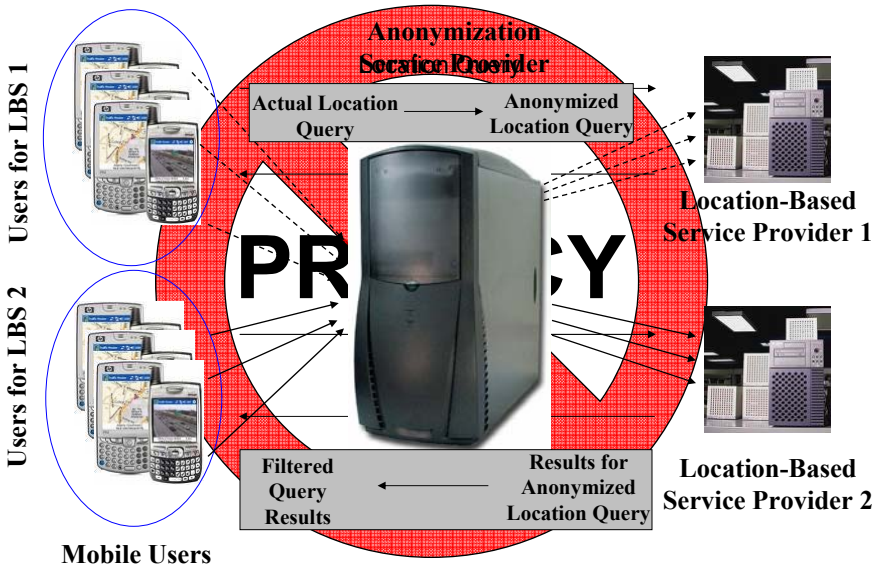
- **Adversary knows some locations of the targeted user**
- Even different pseudonyms are used in different queries/updates
- Analyzing the overlapping spatial or temporal windows of two or more consecutive cloaked location queries/updates
- Adversary can infer the linkage of location with the targeted identifier
- Example:
  - **A cloaked spatial region covering an area (user A, B, C,D) overlaps with another cloaked area (users B, C, D, E)**
  - **an adversary can easily link E to the smaller spatial region that violates the minimum spatial resolution and location k-anonymization constraints.**



Open Issue (3): General Framework for Anonymous location query processing

- Transforming original location query to cloaked location query ensure the answer to the actual query is included.
- Extending existing spatial query processing techniques to handle
  - Cloaked range queries
    - Find gas stations 5 miles to this cloaked area
  - Cloaked kNN Queries
    - Find the nearest 5 gas stations to this cloaked area
- See Casper for an example [MokbelChowAref+vldb06]

Location Anonymization: Why & How



Thank You

References

1. Linda Ackerman, James Kempf, and Toshio Miki. Wireless location privacy: A report on law and policy in the united states, the european union, and japan. Technical Report DCL-TR2003-001, DoCoMo Commuinication Laboratories, USA, 2003.
2. Mikhail J. Atallah and Keith B. Frikken. Privacy-Preserving Location-Dependent Query Processing. In Proceeding of the IEEE/ACS International Conference on Pervasive Services, ICPS, pages 9–17, Beirut, Lebanon, July 2004.
3. J. Al-Muhtadi, R. Campbell, A. Kapadia, M.D. Mickunas and S. Yi. Routing through the mist: Privacy preserving communication in ubiquitous computing environments. International conference on Distributed Computing Systems, 2002.
4. P. Bahl and V.N. Padmanabhan. RADAR: An in-building RF-basd user location and tracking system. IEEE INFOCOM, 2000.
5. Bhuvan Bamba and Ling Liu. PrivacyGrid: Location Anonymization Using Hierarchical Grids. Technical Report. June 2007, Georgia Tech.
6. Louise Barkhuus and Anind K. Dey. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In Proceeding of the IFIP Conference on Human-Computer Interaction, INTERACT, pages 709–712, 2003.
7. Alastair R. Beresford. Location Privacy in Ubiquitous Computing. PhD thesis, University of Cambridge, Cambridge, UK, January 2005.
8. Alastair R. Beresford and Frank Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46–55, 2003.
9. Claudio Bettini, Xiaoyang Sean Wang, and Sushil Jajodia. Protecting Privacy Against Location-Based Personal Identification. In Proceeding of the VLDB Workshop on Secure Data Management, SDM, pages 185–199, 2005.
10. Anuket Bhaduri. User Controlled Privacy Protection in Location-based Services. Master's thesis, Department of Spatial Information Science and Engineering, University of Maine, Orono, ME, 2003.

References

1. Nabil Adam and John Worthmann. Security-control methods for statistical databases: a comparative study. ACM Computing Surveys, 1989, 21(4).
2. Rakesh Agrawal and Ramakrishnan Srikant. Privacy-preserving data mining. ACM SIGMOD 2001
3. Dakshi Agrawal and Charu C. Aggarwal. On the desigb and quantification of privacy preserving data mining algorithms. ACM SIGMOD 2001.
4. Tele Atlas North Amercia, Inc. Geocode Website. http://www.geocode.com/, oct. 2002.
5. Allan J. Brimicombe. GIS: Where are the frontiers now? In Proceedings GIS 2002, pages 33–45, 2002.
6. Anuket Bhaduri and Harlan J. Onsrud. User Controlled Privacy Protection in Location-based Services. In International Conference on Geographic Information Science, GIScience, 2002.
7. Philip E. Age. Transport informatics and the new landscape of privacy issues. Computer Professionals for Social Respinsibility (CPSR) newsletter, 13(3), 1995.
8. N. Borisov, I.Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. ACM MobiCom, 2001.
9. Keke Chen and Ling Liu. Towards Attack-Resilient Geometric Data Perturbation, Proceedings of the 7th SIAM (Society for Industrial and Applied Mathematics) International Conference on Data Ming (SDM 2007), to be held in Minneapolis, Minnesota, April 26-28, 2007.
10. Keke Chen and Ling Liu. A Random Rotation Perturbation Approach to Privacy Preserving Data Classification, *Proceedings of the Third IEEE International Conference on Data Mining* (ICDM'05), New Orleans, Louisiana, U.S.A., November 27-30, 2005.

References

11. Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar. Preserving User Location Privacy in Mobile Data Management Infrastructures. In Proceedings of Privacy Enhancing Technology Workshop, PET, 2006.
12. Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu. A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services. In Proceedings of the ACM Symposium on Advances in Geographic Information Systems, ACM GIS, Arlington, VA, November 2006.
13. CNN. Will GPS tech lead to 'geoslavery'? http://www.cnn.com/2003/TECH/ptech/03/11/geo.slavery.ap/ March, 11, 2003.
14. Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location Disclosure to Social Relations: Why, When, and What people Want to Share. In Proc of the International Conference on Human Factors in Computing Systems, CHI, 81–90, 2005.
15. J, Cuellar, J. Morris, and D. Mulligan. Internet Engineering Task Force geopriv requirements. http://www.ietf.org/html.characters/geopriv-charter.html, Oct. 2002.
16. George Danezis, Stephen Lewis, and Ross Anderson. How Much is Location Privacy Worth? In Fourth Workshop on the Economics of Information Security, WEIS, 2005.
17. Victor Teixeira de Almeida and Ralf Hartmut G¨uting. Supporting Uncertainty in Moving Objects in Network Databases. In Proceedings of the ACM Symposium on Advances in Geographic Information Systems, ACM GIS, pages 31–40, Bremen, Germany, November 2005.
18. Jing Du, Jianliang Xu, Xueyan Tang, and Haibo Hu. iPDA: Enabling Privacy-Preserving Location-Based Services. In Proc of the International Conference on Mobile Data Management, MDM, 2007.
19. Matt Duckham and Lars Kulik. A Formal Model of Obfuscation and Negotiation for Location Privacy. In Pervasive, pages 152–170, 2005.
20. Sastry Duri, Jeffrey Elliott, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang. Data Protection and Data Sharing in Telematics. Mobile Networks and Applications, 9(6):693–701, 2004.

References

21. Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang. Framework for Security and Privacy in Automotive Telematics. In Proceeding of the International Workshop on Mobile Commerce, WMC, pages 25–32, September 2002.
22. D. Eastlakem S. Croker and J. Schiller. RFC 1750: Randomness recommendations for security. http//www.ietf.org/rfc/rfc1750.txt, Dec. 1994.
23. Ian Elcoate, Jim Longstaff, and Paul Massey. Location Privacy in Multiple Social Contexts. In Workshop on Privacy, Trust and Identity Issues for Ambient Intelligence, May 2006.
24. A. Fasbender, D. Kesdogan and O. Kubitz. Analysis of security and privacy in mobile IP. Int. Conf. on Telecommunication Systems Modeling and Analysis. Mar 1996.
25. I. Getting. The global positioning system. IEEE Spectrum. 30(12): 36-47, Dec. 1993.
26. Bugra Gedik and Ling Liu. Location Privacy in Mobile Systems: A Personalized Anonymization Model. In Proceeding of the International Conference on Distributed Computing Systems, ICDCS, pages 620–629, 2005.
27. Bugra Gedik and Ling Liu. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. IEEE Transactions on Mobile Computing.
28. Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. MOBIHIDE: A Mobile Peer-to-Peer System for Anonymous Location-Based Queries. In Proceedings of the International Symposium on Advances in Spatial and Temporal Databases, SSTD, 2007.
29. Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. PRIVE: Anonymous Location based Queries in Distributed Mobile Systems. In Proceedings of International Conference on World Wide Web, WWW, pages 1–10, 2007.
30. D. Goldberg, M. Reed and P. Syverson. Onion routing for anonymous and private internet connections. CACM 1999.

References

31. Andreas Gorlach, Andreas Heinemann, and Wesley W. Terpstra. Survey on Location Privacy in Pervasive Computing. In Workshop on Security and Privacy in Pervasive Computing, April 2004.
32. Marco Gruteser and Dirk Grunwald. A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks. In Proceedings of the International Conference on Security in Pervasive Computing, SPC, pages 10–24, 2003.
33. Marco Gruteser and Dirk Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In Proceedings of the International Conference on Mobile Systems, Applications, and Services, MobiSys, pages 163–168, 2003.
34. Marco Gruteser and Baik Hoh. On the Anonymity of Periodic Location Samples. In Proceeding of the International Conference on Security in Pervasive Computing, 2005.
35. Marco Gruteser and Xuan Liu. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security and Privacy, 2(2):28–34, March 2004.
36. Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald. Privacy-Aware Location Sensor Networks. In Proceedings of the Workshop on Hot Topics in Operating Systems, HotOS, pages 163–168, 2003.
37. Y. Huan, X. Fu, Richardo Bettati, and Wei Zhao. A quantitative analysis of anonymous communications. IEEE Transactions on Reliability. 2004.
38. Carl A. Gunter, Michael J. May, and Stuart G. Stubblebine. A Formal Privacy System and Its Application to Location Based Services. In Proceedings of Privacy Enhancing Technology Workshop, PET, pages 256–282, 2004.
39. Andy Harter, Andy Hopper, and Pete Steggles, Andy Ward, and Paul Webster. The anatomy of a context-aware application. ACM MobiCom 1993 pp270-183.
40. Urs Hengartner and Peter Steenkiste. Access Control to Information in Pervasive Computing Environments. In Proceeding of the Workshop on Hot Topics in Operating Systems, pages 157–162, 2003.

References

41. Urs Hengartner and Peter Steenkiste. Protecting Access to People Location Information. In Proceeding of the International Conference on Security in Pervasive Computing, SPC, pages 25–38, 2003.
42. P.A. Karger and Y. Frankel. Security and privacy threats to ITS. Proceedings of the 2nd World Congress on Intelligent Transport Systems. Vol5. Japan. 1995.
43. D. Kesdoganm H, Federrath, A. Jerichow, and A. Pfitzmann. Location management strategies increasing privacy in mobile communications. 12th Inf. Information Security Conference, Greeece, 1996. Chapman & Hall.
44. Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias. Preserving Anonymity in Location Based Services. Technical Report TRB6/06, Department of Computer Science, National University of Singapore, 2006.
45. Hidetoshi Kide. Location Anonymization for Protecting User Privacy in Location-based Services. Master's thesis, School of Information Science and Technology, Osaka University, Japan, 2006.
46. Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh. An Anonymous Communication Technique using Dummies for Location-based Services. In Proceedings of IEEE International Conference on Pervasive Services, ICPS, pages 88–97, 2005.
47. Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Enhancing Security and Privacy in Traffc-Monitoring Systems. IEEE Pervasive Computing Magazine (Special Issue on Intelligent Transportation Systems), 5(34):38–46, 2006.
48. Jason I. Hong and James A. Landay. An Architecture for Privacy-Sensitive Ubiquitous Computing. In Proceedings of The International Conference on Mobile Systems, Applications, and Services, MobiSys, pages 177–189, 2004.
49. Haibo Hu and Dik Lun Lee. Range Nearest-Neighbor Query. IEEE Transactions on Knowledge and Data Engineering, TKDE, 18(1):78–91, 2006.
50. Internet Draft. Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information. http://www.ietf.org/internet-drafts/draft-ietf-geopriv-policy-11.txt, February 2007.

References

51. Internet Engineering Task Force (IETF). Geographic Location/Privacy (geopriv) Workgroup. http://www.ietf.org/html.charters/geopriv-charter.html.
52. Iris A. Junglas and Christiane Spitzmuller. A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services. In Proceeding of the Hawaii International Conference on System Sciences, HICSS, January 2005.
53. Eija Kaasinen. User needs for location-aware mobile services. Personal and Ubiquitous Computing, 7(1):70–79, 2003
54. Tobias K¨olsch, Lothar Fritsch, Markulf Kohlweiss, and Dogan Kesdogan. Privacy for Profitable Location Based Services. In Proceeding of the International Conference on Security in Pervasive Computing, SPC, pages 164–178, 2005.
55. Jiejun Kong, Xiaoyan Hong, M. Y. Sanadidi, and Mario Gerla. Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing. In Proceedings of the IEEE Symposium on Computers and Communications, ISCC, pages 57–62, 2005.
56. Marc Langheinrich. Privacy by design – principles of privacy aware ubiquitous systems. Ubicom 2001 LNCS 2201. 2001 Springer.
57. Iosif Lazaridis and Sharad Mehrotra. Approximate Selection Queries over Imprecise Data. In Proc of the International Conference on Data Engineering, ICDE, pages 140–152, Boston, MA, 2004.
58. Scott Lederer, Jennifer Mankoff, and Anind K. Dey. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In Proceeding of the Extended abstracts of the Conference on Human Factors in Computing Systems, CHI Extended Abstracts, pages 724–725, 2003.
59. Location privacy protection act of 2001. us congress, sponsor: Sen. john edwards(d-nc), http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp, 2001.
60. Zhen Xiao Xiaofeng Meng and Jianliang Xu. Quality-Aware Privacy Protection for Location-Based Services. In Proceedings of the International Conference on Database Systems for Advanced Applications, DASFAA, Bangkok, Thailand, April 2007.

References

61. Mohamed F. Mokbel. Privacy in Location-Based Services: State of Art and research directions. In MDM 2007.
62. Mohamed F. Mokbel, Chi-Yin Chow, and Walid G. Aref. The New Casper: Query Processing for Location Services without Compromising Privacy. In Proceedings of the International Conference on Very Large Data Bases, VLDB, pages 763–774, Seoul, Korea, September 2006.
63. G. Myles, A. Friday, and N. Davies. Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing, 2(1):56–64, 2003.
64. Jinfeng Ni, Chinya V. Ravishankar, and Bir Bhanu. Probabilistic Spatial Database Operations. In Proceedings of the International Symposium on Advances in Spatial and Temporal Databases, SSTD, pages 140–158, Santorini Island, Greece, July 2003.
65. Kari Oinonen. Privacy guidlines. Technical Report LIF TR-101, Location Inter-operability Forum (LIF) -Currently known as Open Mobile Alliance, http://www.openmobilealliance.org/tech/affiliates/lif/lifindex.html, September 2002.
66. Andreas Pfitzmann and Marit Kohntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, pages 1–9, 2000.
67. \Dieter Pfoser and Christian S. Jensen. Capturing the Uncertainty of Moving-Object Representations. In Proceedings of the International Symposium on Advances in Spatial Databases, SSD, pages 111–132, Hong Kong, July 1999.
68. Dieter Pfoser, Nectaria Tryfona, and Christian S. Jensen. Indeterminacy and Spatiotemporal Data: Basic Definitions and Case Study. GeoInformatica, 9(3):211–236, September 2005.
69. N. Priyantha, A. Chakraborty and Hari Balakrishnan. The Cricket location support system. ACM MobiCom 2000.
70. J. Reed, K. Krizman, B. Woerner, and T. Rappaport. An Overview of the Challenges and Progress in Meeting the E-911 Requirement for Location Service. IEEE Personal Communications Magazine, 5(3):30–37, April 1998.

References

71. Michel K. Reiter and Aviel Rubin. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1(1), 1998.
72. RFC 3693. Geopriv Requirements. http://www.ietf.org/rfc/rfc3693.txt, February 2004.
73. RFC 3694. Threat Analysis of the Geopriv Protocol. http://www.ietf.org/rfc/rfc3694.txt, February 2004.
74. P. Samarati and L. Sweeney. Protecting Privacy when disclosing generalization and supression. Tech report SRI-CSL-98-04. CS Lab. SRI International 1998.
75. Hanan Samet. The design and analysis of Spatial Data Structures. Addison-Wesley, 1990.
76. Bill Schilit, Jason Hong, Marco Gruteser. Wireless Location Privacy Protection. December 2003 IEEE Internet Computing.
77. Clay Shields and Brian Neil Levine. A protocol for anonymous communication over the internet. ACM CCS 2000.
78. Asim Smailagic and David Kogan. Location Sensing and Privacy in a Context-aware Computing Environment. IEEE Wireless Communication, 9(5):10–17, 2002.
79. Ian Smith, Anthony LaMarca, Sunny Consolvo, and Paul Dourish. A Social Approach to Privacy in Location-Enhanced Computing. In Proceeding of the Workshop on Security and Privacy in Pervasive Computing, 2004.
80. Einar Snekkenes. Concepts for Personal Location Privacy Policies. In Proceedings of the ACM Conference on Electronic Commerce, pages 48–57, 2001.
81. Mike Spreitzer and Marvin Theimer. Providing location information in a ubiquitous computing environment. (panel discussion). ACM SOSP 1993.
82. The New Standard. GPS Surveillance Creeps into Daily Life. http://newstandardnews.net/content/?action=show item&itemid=3886 November, 14, 2006.

References

83. Yufei Tao, Dimitris Papadias, and Qiongmao Shen. Continuous Nearest Neighbor Search. In Proceedings of the International Conference on Very Large Data Bases, VLDB, pages 287–298, Hong Kong, August 2002.
84. Goce Trajcevski, OuriWolfson, Klaus Hinrichs, and Sam Chamberlain. Managing Uncertainty in Moving Objects Databases. ACM Transactions on Database Systems , TODS, 29(3):463–507, September 2004.
85. Goce Trajcevski, Ouri Wolfson, Fengli Zhang, and Sam Chamberlain. The Geometry of Uncertainty in Moving Objects Databases. In Proceedings of the International Conference on Extending Database Technology, EDBT, pages 233–250, Prague, Czech Republic, March 2002.
86. U.S. Geological Survey (USGS). Digital line graph data. http://edc.usgs.gov/geodata/, oct. 2002
87. U.S. Geological Survey (USGS). Spatial data transfer standard. http://mcmcweb.er.usgs.gov/sdts., 1995.
88. John Voelcker. Stalked by Satellite. IEEE Spectrum, 43(7):15–16, 2006.
89. Roy Want, Andy Hopper, Veronica Falco and Jonathan Gibbons. The active badge location system. ACM transactions on Information Systems (TOIS), 10(1), 1992.
90. Jay Warrior, Eric McHenry, and Kenneth McGee. They Know Where You Are . IEEE Spectrum, 40(7):20–25, 2003.
91. James C. White. People, Not Places: A Policy Framework for Analyzing Location Privacy Issues. Master's thesis, Terry Sanford Institute of Public Policy, Duke University, Durham, NC, 2006.
92. The Wifi Weblog. Companies Increasingly Use GPS-Enabled Cell Phones to Track Employees. http://wifi.weblogsinc.com/2004/09/24/companies-increasingly-use-gps-enabled-cell-phones-to-track/ September, 24, 2004.

References

93. The Wifi Weblog. Companies Increasingly Use GPS-Enabled Cell Phones to Track Employees. http://wifi.weblogsinc.com/2004/09/24/companies-increasingly-use-gps-enabled-cell-phones-to-track/ September, 24, 2004
94. Ouri Wolfson and Huabei Yin. Accuracy and Resource Concumption in Tracking and Location Prediction. In Proceedings of the International Symposium on Advances in Spatial and Temporal Databases, SSTD, pages 325–343, Santorini Island, Greece, July 2003.
95. Mahmoud Youssef, Vijayalakshmi Atluri, and Nabil R. Adam. Preserving Mobile Customer Privacy: An Access Control System for Moving Objects and Customer Profiles. In Proceedings of the International Conference on Mobile Data Management, MDM, pages 67–76, 2005.
96. ZDNet. Car spy pushes privacy limit. http://news.zdnet.com/2100-9595 22-530115.html. June, 19, 2001.
97. Jianjun Zhang, Gong Zhang, Ling Liu. GeoGrid: A Scalable Location Service Network. Proceedings of 27th IEEE International Conference on Distributed Computing Systems (ICDCS 2007).