**Table of Contents**

1.Introduction……………………………………………………….....................1

1.1 Problem Statement……………………………………………………1

1.2 Objectives……………………………………………...........................1

2.Existing Methods……………………………………………………………...3

2.1 Trusted Third Party (TTP) Based……………………...........................3

2.1.1. Cache Based Spatial Query Processing………………………3.

2.2 Trusted Third Party (TTP) Free……………………..............................5

2.2.1 Location Obfuscation…………………………………………5

2.2.2 Client-Server Architecture:False Dummies…………………..7

2.2.3 Location Privacy in Location Based Services…………………8

2.2.4 A Peer to Peer(P2P) Spatial Cloaking Algorithm ……………..9

2.2.5 Three Dimensional Access Control Model……………………………..11

3.Comparison……………………………………………………………………………………………………12

4.Conclusion……………………………………………………………………..13

5.References……………………………………………………………………...14

List of Tables

1. Comparison**…………………………………………………………..…12**

**List of Figures**

system architecture ………………………………………………………………..3

Dynamic allocation of cache space based on spatial query frequency. ………….4

Idealized Example of an obfuscated location based information service ………...5

.Obfuscation Graph……………………………………………………………… 6

Representation of continuous Cartesian space using discrete distance-weighted graphs…………………………………………………………………………….. 6

Client Server Model With False Dummies ……………………………………….7

P2P spatial cloaking algorithm…………………………………………………..10

**List of Acronyms**

TTP:Trusted Third Party

LBS:Location Service Provider

P2P :Peer To Peer

AWN:Adhoc Wireless Network

PH=Privacy Homomorphism

PKI=Public Key Infrastructure

TPLBSP=Third-Party Location Based Service Provider

**Abstract**

*Location-based services (LBS) are a general class of computer program-level services that use location data to control features .i.e.,Foursquare,Facebook.. Main pitfall of LBS service provider is that it is not trusted. Adverseries can use user physical location in wrong way .So our main concern is maintaining privacy in location based services so that users can use LBS services without any fear of unfolding their privacy. We are here for discussing main algorithm proposed for maintaining privacy in Location Based Services for mobile users And summarizes the pitfalls and usefulness of each particular algorithm and reached at a conclusion that TTP-free is more secure than TTP-Based.*

***Keywords-*** TTP-Free,TTP-Based

**Chapter** 1

Introduction

1.1 Problem Statement

Location-based services (LBS)—applications that provide information to users based on their location are a growing business. From social networking to navigation to banking, consumers are being offered a range of new location-based services. But every time a consumer uses one of these services, there is a risk that the company offering the service may be collecting and retaining detailed records of who she is, where she goes, and what she does. Once collected, outdated privacy laws and varying corporate practices can leave this sensitive information vulnerable to access by the government and third parties. What are the privacy implications of LBS, and how can businesses, policymakers, public interest groups,and consumers work together to update the laws and create stronger policies so that consumers can feel confident using these services?

1.2 Objectives

LBS are rapidly expanding in both number and variety. They offer a wide range of services: navigation tools to help you reach your destination (e.g., MapQuest); local search to help you find nearby businesses or events (e.g., Yelp); friend-finders and social networking (e.g., Loopt and Google Buzz); applications that allow you to “check in” at certain locations (e.g., foursquare); and applications that can link your location to other activities (e.g., Twitter and Facebook). Many users currently access LBS through mobile phones, but location-aware devices such as laptop and desktop computers, iPads, and in-car navigation and assistance systems can also be used to access many of these services.

LBS offer tailored services that respond as you move from one place to another. But by using LBS,consumers may unknowingly allow companies to compile detailed profiles of their lives: the places they visit, the events they attend, the people they meet, and more. And if LBS assemble these consumer profiles, other parties—especially the government—may be eager to access this sensitive personal information. Americans should not be forced to choose between using new technology and keeping control of the private details of their lives. Instead, they have the right to expect that new technologies will improve their lives without invading their privacy.

Unfortunately, legal protections have not kept pace with technological change.Constitutional privacy protections have yet to account for the fact that LBS are capable of generating detailed records that may reveal intimate and personal facts about a person’s life, facts that are rightly considered private. Existing privacy statutes were written decades ago, before LBS even existed. And many LBS privacy policies do more to protect company interests than to safeguard consumer privacy. As a result, the privacy protection for information collected, held, and shared by LBS providers is often inadequate or uncertain. As LBS become more popular and more central to the way Americans interact with technology and with each other, ensuring that there are strong and clear protections for the information they collect will be essential to building consumer trust, ensuring the long-term success of LBS, and protecting privacy.

**Chapter 2**

Existing Methods

2.1 Trusted Third Party Based

2.1.1 Cache Based Spatial Query Processing

A. Introduction

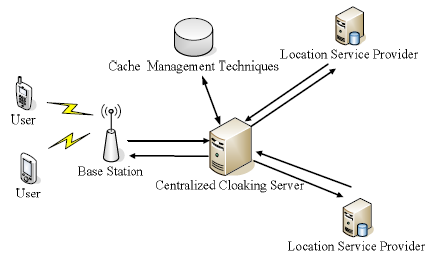
In order to access location-based services, mobile users have to disclose their exact locations to service providers. However, adversaries could collect the location information for purposes against mobile users’ privacy. There are existing solutions for privacy protection by utilizing the K-anonymity model. However, the computational and communication costs arehigh*.* This research proposes cache management techniques for further improving user privacy protection, saving computational power, and decreasing communication costs*.*

B. Type

Trusted Third Party Based (TTP-Based)

C. System Architecture

Our system architecture is consisted of four main entities: mobile users, the location cloaker, cache management techniques, and location-based service providersas illustrated in Figure 1.



**Figure 1. System architecture.**

D. Mechanism

all the spatial queries and returned query results have to pass through the location cloaker. Consequently, if the location cloaker can cache the received query results from service providers, the cached results can be utilized to fulfill new spatial queries from mobile users. By applying this cache based solution, mobile users’ privacy protection can be further improved. Since the location cloaker can solve a certain number of queries without forwarding them to service providers, it would be much more difficult for adversaries to launch correlation attacks.

E. Cache Space Management and Replacement Policies

Time Based Policy

The weight of each grid cell is according to a timer, which records the time interval from the last visit to present. Similar to the Least Recently Used (LRU) algorithm, the cell, which has the largest time interval, will be discarded first.

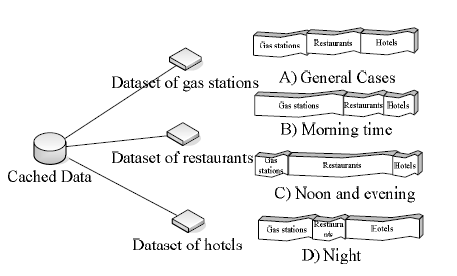
Retrieval Frequency Based Policy

Since retrieval frequency reflects the popularity of a certain data object/spatial region, this method decides the weight of each grid cell based on the number of times which it has been searched. The cell with the lowest visit frequency will be replaced first.

Mobile User Density Based Policy

Mobile users usually interest in POIs close to their current locations. Accordingly, it is an ideal

strategy to keep grid cells which have high mobile user density and discard low user density cells.

.

**Figure 2. Dynamic allocation of cache space based on spatial query frequency.**

2.2 Trusted Third Party Free (TTP\_FREE) Method

2.2.1 A Formal Model of Obfuscation and Negotiation for Location Privacy

A.Introduction

Location aware pervasive computing environments provide the ability to automatically of spatial and temporal precision and accuracy. Location is an especially sensitive sense, communicate, and process information about a person’s location, with a high degree type of personal information, and so safeguarding an individual’s location privacy has become an key issue for pervasive computing research. In our model an individual may deliberately degrade the quality of information about his or her location in order to protect his or her privacy, a process called obfuscation.

B. Type

Trusted Third Party Based (TTP-Based) model.

C. Architecture

The key assumptions made by are architecture are:

– A client device uses some combination of conventional location-sensing techniques to provide precise and accurate information about the client’s location

– That client device is able to communicate directly with a third-party location based service provider (TPLBSP) via a wireless network to obtain some information service based on the client’s current location.

– The information that the client chooses to reveal about his or her location constitutes the only source of information available to the TPLBSP about that client’s location.

D. Mechanism

This section aims to provide a concise formal model of obfuscation and location privacy**.**

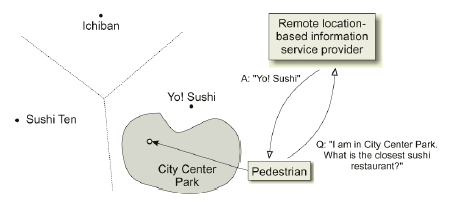
****

Figure 3.Idealized Example of an obfuscated location based information service

Obfuscation Model

Geographic Space

As a first step, we adopt a discrete model of geographic space as a graph, *G =*(*V,E).* Thus,geographic locations are modeled as a set of vertices, V , with connectivity or adjacency between pairs of locations modeled as a set of edges E, where E ⊆ V × V.

Obfuscation in a Graph

An individual’s location in geographic space is represented as a vertex *l ∈ V .*An obfuscation of an individual’s location l is represented as a set O, such that l ∈ O and O⊆V.

# C:\Users\sawan\Downloads\Project\5\p5.png

Figure 4. Graph *G* = (*V,E*) with example obfuscation *O* = *{a, c, h, m, n, o,w}* (black vertices)

E. Proximity Location-Based Services

A simple but important subclass of location-based services concerns querying a spatial database in order to find information about features of interest that are nearest to an individual’s location, which we refer to as *proximity queries.* Examples of such queries include, “With reference to my current location, – “what is the address of the closest sushi restaurant?”

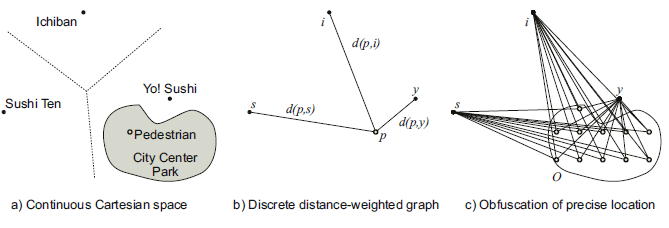
****

Fig. 5. Representation of continuous Cartesian space using discrete distance-weighted graphs

2..2.2 Client-Server Architecture(TTP-Free): False Dummies

A. Introduction

We propose a new anonymous communication technique to protect the location privacy of people using LBSs. In our proposed technique, a user sends true position data with several false position data (dummies) to a service provider,who creates a reply message for each received position data.The user only extracts the necessary information from the reply message. In this manner, service providers cannot distinguish true position data from a set of position data if all dummies have temporal consistency.

B. Type

Trusted Third party Based (TTP-Based) model

C. Mechanism

A user sends *m* locations, only one of them is true while *m-1* are false dummies

* The server replies with a service for each received location
* The user is the only one who knows the true location, and hence the true answer
* Generating false dummies should follow a certain pattern similar to a user pattern but with different locations

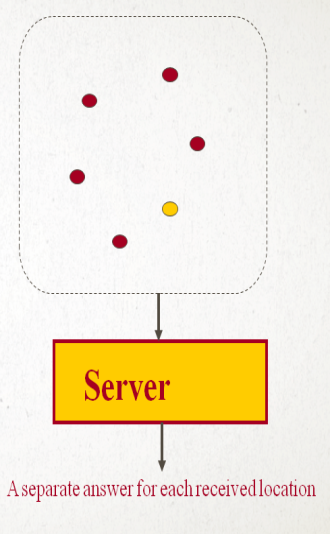
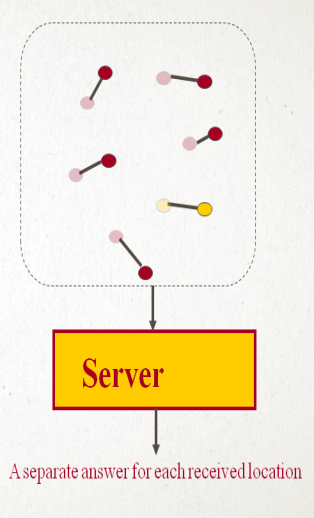
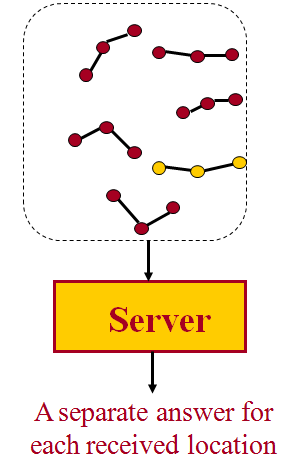


Figure 6: Client Server Model With False Dummies

2.2.3 Location Privacy in Location Based Services

A. Introduction

It does not rely on trusted third parties such as an anonymiser.It is a distributed solution. The k-anonymised locations are obtained by the collaboration of the users in a cloaking region.It is a modular solution. Depending on the privacy requirements of the users, they can use different modules. When the complete solution is used, it guarantees the privacy location of the users even when malicious collusions exist. The location information of the anonymised users cannot be disclosed by the peers, nor by the LBS provider.

B. Mechanism

It is introduced step by step, from the simplest version to the most complex and robust one.

Module 1

Basic simple scheme (Messeges with Plain Text).

It is simplest scheme without masking of locations. On request of main user U ,the other (k-1) companions send their real locations to U. The user U then calculates centroid of k-locations and send it to other (k-1) companions. They can use this centroid for their location based services.

The drawback of this scheme is if U is a malicious user then the locations of other comapanions are disclosed to U and it can be used in harmful ways.

Module 2

Masking Locations (Real locations with Gaussian noise)

In order to prevent U from knowing real locations of companions, it adds the Gaussian noise with null average in computation of centroid scheme. Every user sends the masked location calculated by adding real locations and Gaussian pseudo-random number to U. The user U calculates centroid of masked locations and send it to other (k-1) companions. They can use this centroid for their location based services.

Unfortunately this approach has a limitation.Due to the use of Gaussian noise with null average,users should not use this technique repeatedly without changing their real locations because the cancellation of added noise.

Module 3

Public key Privacy Homomorphism (PH)

It assumes that there is Public Key Infrastructure(PKI) supplying to LBS provider P which has two key public key(pk) and secret key(sk). It has two function encryption and decryption with additive polymorphism.

The user U sends request to get locations of (k-1) companions. Each companion Ui makes use of the PKI to request the public key pk of LBS provider Idp. Ui checks the validity of pk and sends U their encrypted masked location messege.U makes use of PKI to request pk and encrypts her/his masked location.U perform addition of locations,although she/he is not able to see them.Now U sends this value to P .P decrypts it by use of sk and obtains masked centroid.It is the only one who knows sk.After this it return query result based on resultant messege.

The drawback of this if U colludes with the P then it can use this information in wrong way.

Module 4

Chain based messege exchange

In this situation we propose to ectend the previous solution with the use of a random-order chain, which determines the order in which the messeges will be exchanged between the users.With this proposal, the messege exchange is no longer centralized by U.On th contarary, the encrypted locations travel along the AWN following a route randomly chosen at every hop.

The goal of the addition of random-order chain in the messege-sending is the avoidance of a centralized collector node. Morever,by allowing a distributed computation of the summation of locations,the protocol becomes more resilient against collution attacks.

2.2.4 Peer to Peer(P2P) Spatial Cloaking Algorithm for Anonymous Location based Services

A. Introduction

In Peer to Peer(P2P) Spatial Cloaking algorithm in which mobile and stationary users can entertain location-based services without revealing their exact location information. The main idea is that before requesting any location-based service, the mobile user will form a group from her peers via single-hop communication and/or multi-hop routing. Then, the spatial cloaked area is computed as the region that covers the entire group of peers. Two modes of operations are supported within the proposed P2P spatial cloaking algorithm, namely, the on-demand mode and the proactive mode. Experimental results show that the P2P spatial cloaking algorithm operated in the on-demand mode has lower communication cost and better quality of services than the proactive mode, but the on-demand incurs longer response time.

B. Mechanism

The main idea is that whenever a user wants to issue a location-based query, the user broadcasts a request to its neighbors to form a group. Then, a random user of the group will act as the query sender.

It operates in three major phases.

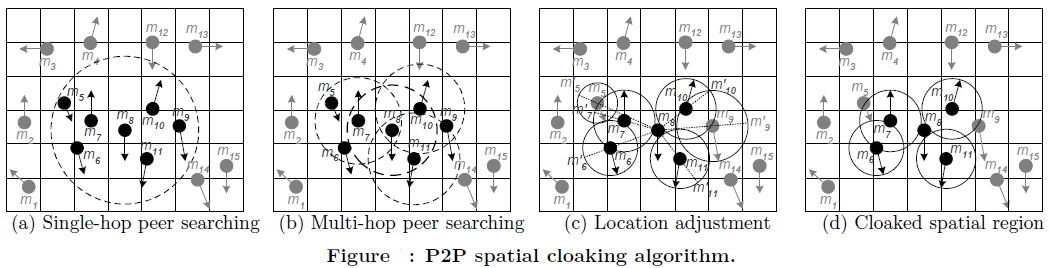


Figure 7

Phase 1

Peer Searching

The user U Broadcast FORM\_GROUP messege with hop distance and hop ID (which is used to distinguish all users).This can be done using singe-hop peer searching /multi-hop peer searching .U waits until the group will become of size k.

Phase 2

Location Adjustment

It is not necessary that user remains static after sending of his/her location. So we may need to calculate the maximum possible distance between U and other peers.For this Ecludean distance formula which is based on maximum possible velocity of peer ,can be used and accordingly location of peer will be adjusted.

Phase 3

Spatial Cloaking

The next step is to blur user location into a region aligned to a grid that cover the k-1 nearest peers so that no one can guess the exact location of peer.

This P2P algorithm can be operated in two modes given below

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.

2.2.5 Three Dimensional Access Control Model

A. Introduction

Privacy protection is a very important issue and solutions must be developed for wide acceptance of location based services (LBSs) in wireless applications. Current approaches rely mostly on the use of privacy policies to describe and solve this problem in an ad hoc way. In this paper, we propose a method based on the three-dimensional access control model to support privacy requirements. We show that our method can better describe and support user location privacy requirements in LBSs.

B. Type

Trusted Third Party Free (TTP-FREE)

C. A Three-Dimensional Access Control Matrix Model

In the traditional access control matrix, S represents the set of subjects, e.g., mobile users, and O represents the set of the objects, e.g., files containing user location information, that need to be properly protected. For privacy protection, we introduce the privacy-concerning subjects S’ to express the set of subjects whose privacy may be affected and thus needs to be protected when any of the objects is accessed.

D. Mechanism

-The server locates in the three-dimensional matrix all the entries corresponding to s and o, i.e., M[s, o,S’], and retrieves all the entries.

The server examines all the retrieved entries to look for the access right that corresponds to read, i.e.,<read, decision>.

If the result is empty, i.e., there is no matrix entry that meets the condition, the request is denied.

-If the result is not empty, at least one of the two entries M[s, o, mother] and M[s, o, father] would contain <read, decision>. If any of the entries has <read, “no”>, the request is denied, that is, subject s is denied of access to the boy’s location information. This situation corresponds to the case in which the boy’s location information is considered to be too sensitive to be disclosed to this particular person represented by subject s.

-Based on the right specification in the two entries M[s, o, mother] and M[s, o, father], the server will initiate some actions, such as querying one or both parents in response to <read, “inquire”>, to ask for real-time approval for granting the access from the parents. A <read, “yes”> immediately leads to an approval.

**Chapter 3**

Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.No | Type | Name | Advantages/Features | Challenges/Limitations |
| 1 | TTP-Based | Location-Obfuscation | -Does not presents a barrier to authentication and personalization  -Provides high-quality information services  -Better option in comparison to anonymity and pseudonymity | -Limited by its fundamentally static nature.  -Difficult to determine what obfuscation will provide the best balance of location privacy  -High cost of calculation |
| 2 | TTP-FREE | Client-Server Architecture: False Dummies | -Provides high-quality information services using low-quality positional information  - locations Does not require trusted third party anonymizer that maintains all user | - This model of location privacy is limited by its fundamentally static nature |
| 3 | TTP-FREE | Location Privacy in Lbs | -It is not centralized but distributed;  -It is robust against the collusion of a malicious user and a service provider;  -Due to its modularity, users can utilize the modules that they really need depending on their current needs. | -Not efficient in some situations in which the number of malicious users is greater than one. |
| 4 | TTP-FREE | P2P Spatial Cloaking Algorithm for Anonymous Lbs | -It doesn’t rely on third trusted party;  -Flexibility on selection of two different modes (i.e. On-demand mode , Proactive mode) | -Some performances issues are there for both modes  For example, in On-demand response time is more than proactive mode and Proactive mode generally incurs higher communication overhead. |
| 5 | TTP-FREE | Three Dimensional Access control model | -Allow access control to any number of users.  -User can decide whether and under what condition information is disclosed.  -Support any type of privacy requirement.  Can be applied to wireless services in which privacy is a seriousconcern. | -Three dimensional storage is somewhat cumbersome.  -More space required. |
| 6 | TTP-Baesd | Cache Based Spatial Query Processing | -Saving computational power  -Decreasing communication costs.  -User privacy protection can be further improved , because the trusted server does not have to forward every query to service providers. | -Initially ,cache hit ration is small, so does not sure privacy.  -Quality depend on third party. |

**Chapter 4**

Conclusion

After comparison analysis of every major and minor aspects of Trusted Third Party (TTP) Based model and Trusted Third Party Free model of algorithms and architecture proposed for enhancing privacy in location based services, We have reached the conclusion that Trusted Third Party Free model (TTP-FREE) is more sophisticated, Reliable and can be a major forwarding footsteps to ensure security in location Based Services without any overhead of indulging Third party.

References

[1] Fei Xu, Jingsha He, Xu Wu, Jing Xu,”A Method for Privacy Protection in Location Based Services”, IEEE Ninth International Conference on Computer and Information Technology,2009.

[2] Agusti Solanas \*, Antoni Martı´nez-Balleste,” A TTP-free protocol for location privacy in location-based services”,2008.

[3] Yu Chen1 Jie Bao2 Wei-Shinn Ku2 Jiun-Long,” Cache Management Techniques for Privacy Preserving Location-based Services”,2008.

[4]Mohamed F. Mokbel and Chi-Yin Chow. “Challenges in Preserving Location Privacy in Peer-to-Peer Environments” . In Proceedings of the International Workshop on Information Processing over Evolving Networks, WINPEN, Hong Kong, June 2006.

[5]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.

[6] Matt Duckham and Lars Kulik , “LNCS 3468 - A Formal Model of Obfuscation and Negotiation for Location Privacy “,2005.

[7]The Guardian Unlimited. How I stalked my girlfriend. Available:http://technology.guardian.co.uk/news/story/0,,1699156,00.html February, 1, 2006.

[8] G. Myles, A. Friday, and N. Davies. “Preserving Privacy in Environments with Location-Based Applications”, IEEE Pervasive Computing, 2(1):56–64, 2003.

[9]CNN. Will GPS tech lead to ’geoslavery’?, Available:http://www.cnn.com/2003/TECH/ptech/03/11/geo.slavery.ap/ March, 11, 2003.

[10]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.

[11] Location-based service ,Available: http://en.wikipedia.org/wiki/Location-based\_service.