International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Exploiting Service Similarity Based on Location Privacy

Pushpalata Bhagadkar[1], Tanuja Dhope[2]

[1]G.H. Raisoni College of Engineering and management, Ahemadnagar, India

[2]G.H. Raisoni College of Engineering and management, Pune, India

Abstract: ***Location based applications exploits the focusing capabilities of mobile device to determine the current position of user, and specifies the query results to capture the neighboring points of interest. As Location knowledge is truly recognized as personal information, One of the immediate issues hampering the wide reception of location-based applications is the defect of appropriate methodologies that gives grain privacy controls to user without affecting the usability of service. In this paper the propose system is an innovative approach that simultaneously ensures both the privacy and the integrity. This is achieved by using space encryption as the basis of our approach and then devising techniques that enable the data users to audit the integrity of the query result for the most important spatial query types: range queries and k -nearest-neighbor queries (k NN). And it can be done by using the MR-tree, an index based on the R*-tree, capable of authenticating arbitrary spatial queries. We can show, analytically and experimentally, that the MR-tree is considerably faster to build and consumes less space. The MR-tree combines concepts from MB and R*-trees.***

Keywords: Privacy-supportive LBS, location privacy, service quality

1. Introduction

Location Based Service (LBS) has become one of the most popular mobile applications due to the wide use of Smartphones [1]. An increasing number of communication devices (e.g., mobile phones, PDAs), feature positioning capabilities (e.g. GPS), Users may ask location-dependent queries, such as “find the nearest Hospital ”, answer of this question is given by Location Based Services (LBS) like Google Maps or Map quest [2]. However, queries may disclose subtle information regarding individuals, including their health condition, their lifestyle habits, political and religious bonding, or may result in gratuitous advertisement (i.e., spam)[2]. Privacy concerns are expected to rise as LBSs become more common. Observe that privacy is not protected by replacing the real user identity with a fake one (i.e., pseudonym), because, in order to process location-dependent queries, the LBS needs the exact location of the querying user[2]. An attacker, which may be the LBS itself, can infer the identity of the query source by associating the location with a particular individual. This can happen in practice, with the use of a public telephone directory, which includes subscribers’ addresses Location based advertising and local search are generating most significant revenues like navigation application and also going forward. The smartphones, equipped with GPS modules, have powerful computation ability to process holders’ location information, and this brought the flood of LBS applications in the smartphone ecosystem. A good example is the smartphone camera: if one takes a photo with a smartphone camera, the location where the photo is taken is embedded in the picture automatically, which helps one’s recognition [1]. Privacy and usability are two equally important requirements for successful realization of a location-based application. Meanwhile, due to the recent advances in wireless technology, mobile devices (e.g., cell phones, PDAs, laptops) with wireless communication capabilities are increasingly becoming popular [3]. Hence, we are presenting the proof of the emergence of many location-based services (LBS) that allow users to issue spatial queries from their mobile devices everywhere. Obviously, these applications require a quality spatial data, and this results in an step by step increase in the customers of spatial data acquirers [3].

In this paper we are going to propose an innovative approach that simultaneously ensures both the privacy and the integrity. This is achieved by using space encryption as the basis of our approach and then devising techniques that enable the data users to audit the integrity of the query result for the most important spatial query types: range queries and k -nearest-neighbor queries (k-NN). Our proposed contribution is the MR-tree, an index based on the R*-tree, capable of authenticating arbitrary spatial queries. We show, analytically and experimentally, that the MR-tree is considerably faster to build and consumes less space. The MR-tree combines concepts from MB and R*-trees.

2. Related Work

In [4] paper ,shown that Users of location-based services (LBSs) may have serious privacy concerns when using these technologies since their location can be utilized by adversaries to infer privacy-sensitive information about them. In this work, we analyze the mainstream anonymity solutions proposed for LBSs based on k-anonymity, and point out that these do not follow the safe assumptions as per the original definition of k-anonymity.

In [5] paper, surveyed that Obfuscation concerns the practice of deliberately degrading the quality of information in some way, so as to protect the privacy of the individual to whom that information refers.

In [6] paper, discussed the increasing trend of embedding positioning capabilities (e.g., GPS) in mobile devices facilitates the widespread use of Location Based Services. For such applications to succeed, privacy and confidentiality are essential. Existing privacy enhancing techniques rely on encryption to safeguard communication channels, and on

pseudonyms to protect user identities. Nevertheless, the query contents may disclose the physical location of the user.

In [8] it is observed that Recently, highly accurate positioning devices enable us to provide various types of location-based services. On the other hand, because such position data include deeply personal information, the protection of location privacy is one of the most significant problems in location-based services. In this paper, we propose an anonymous communication technique to protect the location privacy of the users of location-based services.

3. A Framework for Capturing Location Privacy and Service Quality

Framework contains the description of a system model that connects privacy, service quality and cloaked information. This model is the basis for subsequent discussions. Figure 1 illustrates this system model[4].

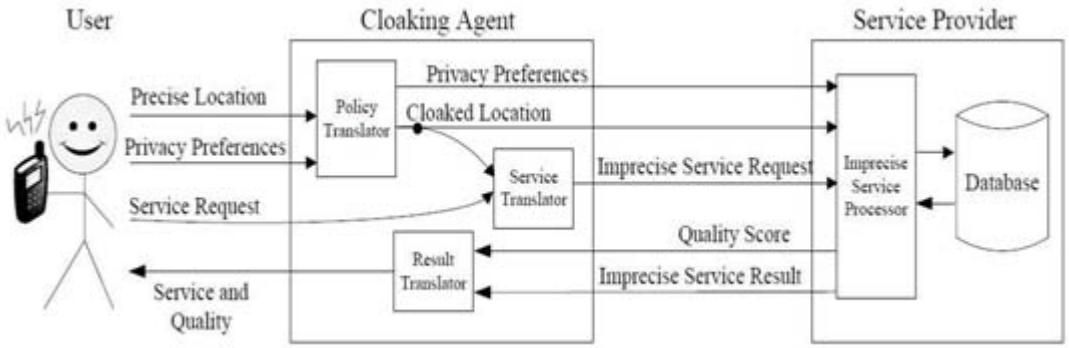
In this main idea is to allow the user to specify it's location, service request and privacy requirements to the cloaking agent. Which then builds the cloaked location (i.e., a larger region that contains the user's true location) and an "imprecise" service request. On collection of this information, the service provider processes the request and sends back the service and feedback to the user. The cloaking agent can either be implemented in the user's device, or provided by a third-party system. In Figure 1 it can be seen that a user can first specify it's privacy preferences through a privacy language. Privacy language, that we are planning to develop, allows a subject to specify her privacy preferences with respect to:

- Locations - a user may specify that when being near to a given object, cloaking is required, and the accuracy requirements. Locations can be logical or physical;
- Other users and service providers - a user may also specify that her presence be made known (or hidden) to specific users and service providers[4].

Inside the cloaking agent, the user's privacy preferences are then forwarded to the policy translator. The policy translator produces a cloaked location based on the precise location of the user and it's privacy requirements. For instance, if the user's requirement is "generate a cloaked location that covers five buildings when I am in Area A", the policy translator produces the corresponding cloaked location when it detects the user is in Area A. The policy translator also forwards to the service provider the user's privacy preference concerning other users and service providers if needs. Based on the cloaked location and the service request, the service translator produces an "imprecise" service request that processes cloaked data. Based on the recommendation from the cloaking agent, the user can then decide if the degree of privacy should be reduced. Let us now focus on data modeling, query evaluation, quality and privacy protection issues for this system. A novel architecture for LBS applications that is directed toward revealing privacy/utility tradeoffs to a user before an actual geotagged query is made. Unlike a typical competitive.architecture where the LBS provider does not actively participate in making privacy decisions, a privacy-supportive LBS as a provider willing to provide supplemental information for making "informed" privacy decisions [4].

4. Privacy-Supportive LBS

There is an increasing doubt about how a LBS provider handles location data. The Location accuracy is indeed a characteristic requirement of the application as a evidence to build an strong market adoption. As only the service provider can maintains the database of queried objects in real time, it is reasonable that differences or similarities in the output of a query can be efficiently computed at the server side. A user is unable to make privacy decisions without this computation. From these comments, a privacy supportive LBS seems both appropriate as well as important. Also it founds that a simple opt-in LBS is not privacy-supportive, as the implications of not using ones geo-location is unavailable to the user.



Managing Privacy and Service Quality with the Cloaking Agent

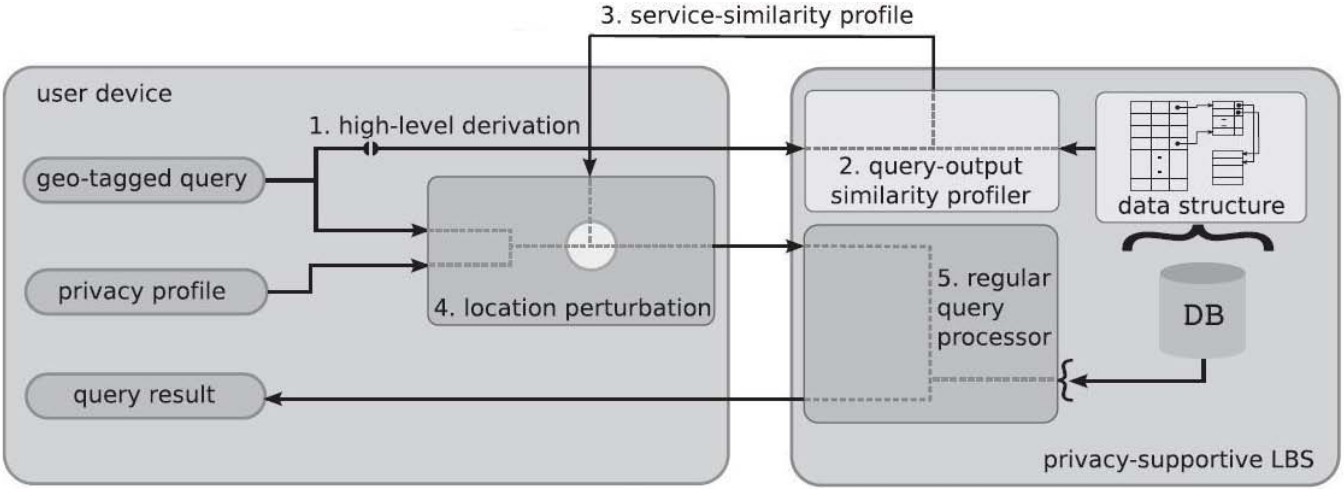


Figure 2: Communication order for a location-based query in the presence of a privacy-supportive LBS

A. Communication Order For a Location Based Query

The communication setting includes one or more users equipped with GPS-enabled devices, and an LBS provider possessing a database of points-of-interest (POI). These POI may be static or dynamic, as in case of local business listings and as in case of a friend-finder service respectively where users usually check-in/out of the underlying on social-networking platform. Like this in almost all operating LBS applications, user access to the service is supplemented by a geographic tag identifying the position of the user. Authentication may or may not be necessary to use the service, since many applications are able to provide a better result set in the latter case. The service itself may have requirement of other parameters to be specified, such as searches keywords or profile descriptions. The geographic tag in the query is typically the GPS-coordinates of the user device, but can also be a carefully designed location.

B. System Architecture

A privacy-supportive LBS architecture employs an intermediate communication with the LBS In the location disclosure mechanism the communication pattern is presented in Fig. 2. The user device forwards the query to the LBS, albeit uses a high-level generalization of the user's geographic location in it. This generalization can be derived as per user-specification, or obtained automatically from the location approximation. A provider can conclude using a cell-towers and Wi-Fi-access point database. As response to this first query phase, the user obtains a service-similarity profile. This profile is a representation of the similarities in the query output of different geographic locations. The exact form taken by this profile, as well as the data structures employed in computing this profile, may vary from application to application.

A location perturbation engine on the user side then determines a noisy location to use based on the user's privacy profile and the retrieved service-similarity profile. The LBS processes the query with respect to the noisy location. A user can manually interact with the service-similarity profile to assess which locations have the highest (or acceptable) level of result set similarity, within the constraints of the location noise she wants to infuse into the query. In this case, a good visualization of the similarity profile is required. Although this is the most flexible method of putting the tradeoff information to use, such high degree of interaction will affect the usability of the application, especially when queries are made frequently. Hence, we assume that action axioms have been provided by the user to make the process automatic. The privacy profile then states how a location is to be selected for different categories of applications, their importance, and the relative location sensitivity. Policy specifications such as these, and their integration into the decision making process, warrant an extensive exploration. We will avoid this frontier in this work. A naive approach is to allow the user to select a location sensitivity level (much like choosing the ringer-state in a mobile phone), assess query result accuracy at the corresponding location granularity the similarity profile), and notify the user if the accuracy (using drops below a threshold. Note that the policy executes within a user's device and reveals little or no information on how locations get chosen.

5. Proposed System

A. Problem Statement

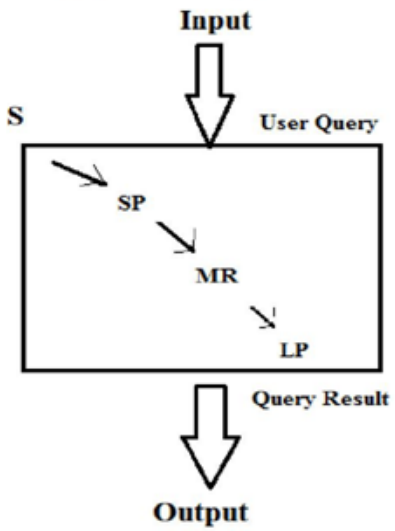
Privacy and usability are two equally important requirements for successful recognition of a location-based application. Privacy (location) is widely defined as a "personally" estimated restriction on when and where someone's position is considered appropriate for disclosure. Existing system searches user query locally using data structure, so query takes time to search result. Also in existing system there is lack of efficiency and also space and time consuming system.

For fast and efficient searching technique also space efficient we can propose MR-tree. The MR-tree is considerably faster to build and consumes less space. At the same time, it is much more efficient for query processing and verification. Merkletree, which is an authenticated data structure (ADS) that is built on the dataset. Proposed system provides a novel index suitable for location based query search[9].

Let S be the system which use for fine grain privacy controls to a user without vastly affecting the usability of the service.

In this system we proposed a user-centric location based service architecture. We construct a local search application based on MR tree architecture and demonstrate how meaningful information can be exchanged between the user and the service provider.

$S = \{UQ, SP, MR, LP, QR\}$



Where S=System,

UQ=The user device forwards the query to the LBS

SP = Service Similarity Profile, This profile is a representation of the similarities in the query output at different geographic locations

MR = Merkel tree, to develops an authenticated data structure (ADS) called Merkle R-tree (MR-tree) based on R*-tree and Merkle tree.

LP= Location Perturbation

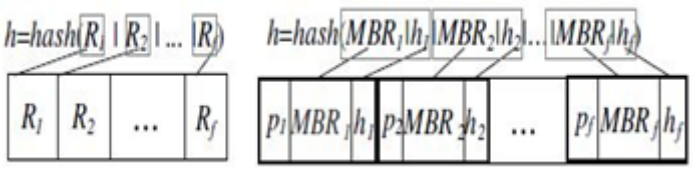
QR=Query Result.

1) UQ (User Query)

The user device forwards the query to the LBS, albeit uses a high-level generalization of the user's geographic location in it. This generalization may be derived as per user-specification (say at the level of the city), or obtained automatically from the location approximation that provider can infer using a cell-towers and Wi-Fi access points database.

2) *MR (Merkle Tree)*

The MR-tree combines concepts from MB and R*-trees the node structure. Leaf nodes are identical to those of the R*-tree: each entry Ri corresponds to a data object. A hash value is computed on the concatenation of the binary representation of all objects in the node. Internal nodes contain entries of the form (*pi*, *MBRi*, *hi*), signifying the pointer, minimum bounding rectangle and hash value of the *i*th child, respectively.



(a) Leaf Node (b) Internal Node

Figure 3:.MR-tree node *structure*

6. Conclusion and Future Scope

This paper presented a novel architecture to help identify privacy and utility tradeoffs in LBS. The architecture has a user-centric design that delays the sharing of a location coordinate until the user has evaluated the impact of its accuracy on the service quality. Also there is a framework with MR-tree for efficient methods. In this paper, we propose the MR-tree, an authenticated index based on the Merkle Hash tree and the R*-tree. Our method outperforms the best current solution by orders of magnitude in many important metrics such as construction cost, index size and verification overhead. Furthermore, we develop a novel synchronized caching protocol, which significantly reduces the communication overhead of the verification step.

References

[1] Xiang-Yang Li and Taeho Jung, "Search…Privacy-preserving Location Query Service" Department of Computer Science, Illinois Institute of Technology, Chicago, ILxli@cs.iit.edu, tjung@hawk.iit.edu
[2] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. 16th Int'l Conf. World Wide Web, pp. 371-380, 2007.
[3] RinkuDewri, Member, IEEE, and RamakrishaThurime" Exploiting Service Similarity for Privacy in Location- Based Search Queries", IEEE , VOL. 25, NO. 2, Feb 2014
[4] M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," Proc. Third Int'l Conf. Pervasive Computing, pp. 152-170, 2005
[5] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Seventh Int'l Conf. Pervasive Computing, pp. 390-397, 2009.
[6] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location-Based Services," Proc. IEEE Int'l Conf. Pervasive Services, pp. 88-97, 2005.
[7] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, [10] J. Sythoff and J. Morrison, Location-Based Services: "Preserving User Location Privacy in Mobile Data Management Infrastructures," Proc. Sixth Workshop Privacy Enhancing Technologies, pp. 393-412, 2006.
[8] H. Zang and J. Bolot, "Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study," Proc. 17th Ann. Int'l Conf. Mobile Computing and Networking, pp. 145-156, 2011.
[9] Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios. Spatial Outsourcing for Location-based Services. In ICDE, pages 1082–1091, 2008.
[10] Market Forecast, 2011-2015, Pyramid Research, 2011.
[11] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Seventh Int'l Conf. Pervasive Computing, pp. 390-397, 2009.
[12] F. Aurenhammer and O. Schwarzkopf, "A Simple On-line Randomized Incremental Algorithm for Computing Higher Order Voronoi Diagrams," Proc. Seventh Ann. Symp. Computational Geometry, pp. 142-151, 1991