International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Location Based Query Processing For Providing Privacy to Exploit Service Similarity: A Survey

Prerana Deokar, Praveen Barapatre

Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala

Professor, Department of Information Technology, SKN Sinhgad Institute of Technology and Science, Lonavala

Abstract: ***Location Based Application(LBA) provide location based services(LBS) by using queries called location based queries(LBQ). The result of these queries is based on location of mobile user. Privacy and Usability are two important issues of realization of location of user queries. Existing established system(s) developing a User Centric location based service architecture(local search application) where a user can observe the impact of inaccuracy on service accuracy before sending request of geo-coordinates to use in request. This article focuses on Location based services and how location based queries are solved using different methods.***

Keywords: Location Based Application(LBA),Location Based Services(LBS),Location Based Queries(LBQ)

1. Introduction

In todays World, Smartphone becomes widely used device. Location of user or object is its geographical position on the earth and such location data is traceable and real time. This information can be catagorized as per longitude , latitude and street address. For location based queries we need to know the geographic domain. Geographic domain is defined by area covered by Mobile Computing Platform.

Paper discusses how location based queries can be solve in efficient manner and provide accuracy to result. Rest of the paper is organized as- second section discusses background of location based queries and their types , third section discusses previous works on location based queries and their merits and demerits. Fourth section discusses conclusion and future work.

2. Background

To understand the location based services we need to know what is exactly geographic domain. A geographic domain is entire area covered by mobile computing platform.

2.1 Location Based Queries

There are four types of location based queries.

2.1.1 Range Query
These queries depends on particular region.Two types of range queries are static range queries and moving range queries.

2.2.2 Nearest Neighbor Query
These queries responsible to retrieve objects to specific locations.

2.2.3 Navigation Query
Navigation queries fetch mobile user path to destination taking network traffic.

2.2.4 Geo-Fence Query
These queries allows user to create virtual boundary on geographic area on the map.

3. Related Work

3.1 Method 1

In paper [1], studies new attack on the anonymity of location data.This paper gives details of privacy model and assumptions.

3.1.1 Anonymous Location Traces
The value of location data dissociated from iden-tity was illustrated in the introduction: a location-based restaurant recommender can offer adequate recommendations based on location and a pseudonymous profile of dining preferences. Many other location-based services (e.g. friend finding services) can similarly operate using a registered pseudonym only, without learning users' real identities. From a technical point of view, location traces can be anonymized or pseudonymized with help from a trusted network proxy. Mobile subscribers, for example, may trust their network provider to forward their location data anonymously to third party location-based service providers.

3.1.2 Threat of re-identification
Golle et al. study the threat of re-identifcation for anony-mous location traces.We focus specifically on the threat of re-identification under the assumption that the approximate home and work locations of the subject can be deduced from the trace (for example with a reverse geocoder). Approxi-mate home and work locations may then be joined with employment directories, tax records or any other public or private dataset available to the adversary to map pairs of home and workplace locations to identities.

3.1.3 Model of privacy
For the sake of example, assume that a subject is the only person in the U.S. who lives in a certain region A and works in a certain region B. The subject's location trace is the only

one with the home/workplace pair (A;B). It does not necessarily follow that the trace can be linked to the subject, as there may be no directory that links the pair (A;B) with the subject's identity. But since the datasets that an adversary may use to re-identify location traces are not known a-priori, it is best to make the most conservative assumptions about them. Accordingly, we assume that if a unique link exists, it will be discovered. Our measure of privacy is the set of all people associated with the pair (A;B), called the anonymity set [8] of the pair. The larger the anonymity set, the larger the crowd one is indistinguishable from, and consequently the better the privacy protection one enjoys. Enlarging the regions A and/or B (e.g. via location obfuscation) increases the size of the anonymity set, and thus the quality of privacy protection.

LEHD origin destination dataset is used.

3.2 Method 2

In paper [2], Call Data Records(CDR) dataset and anonymization techniques are used. A call record is created when a call originates or terminates on the cellular network and it contains various _elds of information regarding that call. We separate the trace into three month-long segments and study them separately. Zang et al process CDRs from each day and identify the locations visited by each user. They create daily location lists for each user with all locations and the number of appearances at that location. Then for each month, we aggregate the daily location lists into a monthly location list and order the locations by the frequency of appearances. Anonymization techniques developed for data query and data publishing.

3.3 Method 3

In paper [3], Basic Spatial Analysis Algorithm is used and this algorithm can be defined by Voronoi diagram. Another algorithm is Negotiation Proximity query with obfuscation. Duckham et al focus on development of following things:
a formal model of obfuscation and location privacy;

- an algorithm for efficient computation of a simple obfuscated location-based service;
- a procedure for achieving a satisfactory balance of location privacy and location-based service quality through negotiation between an individual and a service provider.

3.4 Method 4

This paper [4], proposes anonymous communication techniques to protect location privacy of users of Location Based Services. This paper also describes cost reduction techniques for communication between client and server. At last author conducted performance study experiments. Two types of anonymous communication techniques for Location Based Services
1) Accuracy Reduction
2) Dummy Generation

For Dummy Generation communication technique two algorithms are used i.e. Moving in Neighborhood and Moving in Limited Neighbourhood. This paper also describes the cost reduction techniques. These are Communication technique and Requiring messages respectively.

3.5 Method 5

This paper [5], developed framework for capturing location privacy and service qulity.Also define location cloaking model. This paper describe the threat analysis and solution.

4. Conclusion

Article discusses on location based queries and location based services. Different methods are used for providing location based services.

References

[1] P. Golle and K. Partridge, “On the Anonymity of Home/Work Location Pairs,” Proc. Seventh Int’l Conf. Pervasive Computing, pp. 390-397, 2009.
[2] 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
[3] 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.
[4] H. Kido, Y. Yanagisawa, and T. Satoh, “An Anonymous
[5] Communication Technique Using Dummies for Location-Based Services,” Proc. IEEE Int’l Conf. Pervasive Services, pp. 88-97,2005.
[6] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, “PreservingUser Location Privacy in Mobile Data Management Infrastructures,”Proc. Sixth Workshop Privacy Enhancing Technologies,pp. 393-412, 2006.