Boffin Access

Open Access Journal | Volume: 1.1

Advances in Computer Sciences

ISSN 2517-5718

Privacy Enhancing Grid Based Mechanism for LBS

Rubina Shahin Zuberi*,
Ishrath Fathima,

Department of Electronics & Communication Engineering, Institute of Technology and Science Engineering College, Greater Noida, India

Abstract

Emergence of the growing Location Based Services has a potential barrier of insecurity of users to use it due to privacy concerns. As these services requires, to broadcast constantly the user's locality from untrusted server to get their position based on several services. The user will have privacy issues. LBS require trusted third party server if it is not meant to have peer-peer architecture, limited user's security and large number of interactions. The work presented here implements two minor changes at two levels of LBS provision. The first one is the client's system software based approach which allows no-internet zones as the most privacy protected zones. The second approach makes use of previous techniques of query processing by k anonymising. But by and large works on hierarchical *k* approach based on some intelligent selection by the clients/MOs. The results so far show an improving trend of using t.

Keywords

Location based services (LBS), Moving object {MO}, Trusted Third Party server, *k*-anonymity

Introduction

Our dependency on mobile phones has converged with the computing World more or less into this smart 'always with us' device. The reason is Global data connectivity. Location Based Services (LBS) can be a location finder of the Moving Object (MO), cab finder (may eradicate cab providing services!), friend finder and could even be a family member finder! It can be an informer providing services such as those required for emergencies, fire accidents, traffic conditions, weather reporting, traffic flow information and the likes. Hence LBS are perceived to be an added local network to this global network.

Service providers are needed to deliver the location that the user wants to search. Service providers having a list of nearby hotels, gas stations & restaurants named as Query Points (QP). The database of these query points exposes user's interests at particular times! This can be a privacy threat for most of the users. However many techniques are being developed for preventing the privacy threat pertaining to LBS. There are several levels for application of these methods. The privacy enhancing procedures may be applied at architectural level [1], security providing procedures implemented at hardware as well as software interfaces [2], privacy can be provided at the root of the threats i.e. at the database level through static as well as dynamic DBMS relating to online and offline query tracking [3] and there could be plethora of other ways to incorporate privacy enhancement methods.

This work tries to incorporate and affect most of the perspectives associated with LBS by incorporating the proposed privacy measure to directly affect static as well as dynamic DBMS. Static DBMS relates to the user data generated by the LBS providing server which could be analysed and misused by the privacy attacker. Dynamic DBMS relates to the so called 'live' query data generated resulting into unexpected privacy breach! We have divided the map page generated by the user (for static as well as dynamic database) into grid as done by many previous works [4,5]. Additionally we propose certain minor improvements into the application software of the user's mobiles. Our proposed privacy enhanced system hence incorporates privacy methods primarily on- MOs device software, static and dynamic DBMS at LBS server.

MOs device Software

The application software communicating with LBS server can make some fundamental differences in the way the data bases related to the queries will be generated and hence can inculcate privacy at the primary level of the querying process. This work proposes user settings for identification of high priority areas like home, office or may be few more areas the disclosure of location can become a threat. This process however is not supposed to be mandatory for the user.

Article Information

DOI: 10.31021/acs.20171104
Article Type: Research Article
Journal Type: Open Access
Volume: 1 **Issue:** 1
Manuscript ID: ACS-1-104
Publisher: Boffin Access Limited

Received Date: November 01, 2017
Accepted Date: December 30, 2017
Published Date: February 28, 2018

*Corresponding author:

Rubina Shahin Zuberi
Department of Electronics & Communication Engineering
Institute of Technology and Science Engineering College
Greater Noida
India
E-mail: rshahinz@gmail.com

Citation: Zuberi RS, Fathima I, Privacy Enhancing Grid Based Mechanism for LBS. Int J Surg Proced. 2018 Jan; 1(1):104

Static and Dynamic DBMS

The static data base is supposed to be produced from *k*-nn (nearest neighbours) queries [6,7]. This work considers doing *k*-nn to the cylindrical uncertainty path of the MO's movements [7]. The dynamic or live queries can be, however treated by dividing the map on a simple grid based system and identifying each grid unit by names. These names can be made same or have a possibility of being pseudonymized with the areas whose 95% or more road areas match each other. This grid can be then subdivided and prioritized with the techniques similar to those used in New Casper [8].

Adversarial Models

Few invasions which may be possible with our proposed model at the architectural or DBMS level:-

Timing attack

This is a common attack especially on road networks. Methodologies have been devised to counter the same [9,10]. The problem occurs due to time relation of the movement of MOs. As the interests of user can be tracked on the basis of time period by a well known adversary, this model tries to keep those areas away by prompting the user to send query in a highly sensitive area or not. We propose that user may deactivate the services in these highly sensitive areas to run away completely from such possibilities and can enable it again to liberally use them when he is out of these areas in the first place. When user will start using his LBS just after leaving the sensitive grid areas like home/ office, still there is a possibility of timing attack as the intelligent adversary can breach his privacy correlating the position and time of the MO. Hence our model gives this MO an extra privacy cover by maximising the *k* in the nearest five peripheral grid cells adjacent to the grid area where user has put his LBS off and will gradually decrease the *k* for every subsequent five grid cells. The five grid cells however can be any viable number in accordance with the grid cells and total grid area (figure 1).

Curse of dimensions of the grid cells

If the grid cells are having low dimensions, their *k*-nn queries will obfuscate nicely but as the dimensions of grid cells increases the *k*-nn queries will get more prone to the attacks [11]. The far away MOs will be considered as neighbours and with analysis of different data sets any adversary can make a more precise correlation attack. Hence this model proposes total grid area and number of MOs based dimensions of grid cells.

Internet Protocol localization

The Internet Service Provider (ISP) server may also contain query, time and position stamp of the MO which may be retrieved and misused. Our model, just as in Mix-zones will cut off all data server connections (except allowing the calls from mobile tower) at the chosen high priority locations. Moreover as proposed, the obfuscation level will also remain high in the grid cells near these areas. Hence it will nearly protect user's privacy from these ISP servers as well. The static and dynamic DBMS are also found to give good results by enabling such user generated priorities.

Query server as client

Queries are answered by local servers which may network with the main LBs server. These local query servers may become the source of information for the adversaries. The query server can act as a client to another query server and can generate a dataset. In this model, as the high priority grid cells will be no internet zone with decreasing *k* afterwards, the dataset so generated will be largely secure from the home/ office or high priority grid cells (as per the user's settings).

Traffic flow finger printing

The amount of traffic flow with time stamps is a dataset which can be easily available to the adversary from the traffic monitoring systems releases [12]. These are amongst the main threats of vehicular networks based obfuscation techniques which form the basis of this work. Our procedure of pseudonymizing/ swapping the identified regions on the grid is the first checking measured which is being doubly ensured with the use of signal less high priority areas.

System Design

The proposed model includes two design processes – priority hierarchy settings and static and dynamic query processing.

Priority Hierarchy Settings: Each MO requires the incorporation of option of hierarchy settings of grid area in the device's system software which must be linked to the application software (app in case of mobiles) The settings required to be made by the user initially are identification of the high privacy areas in accordance with his/ her own priorities (which may include home, office etc.).

These settings will deactivate internet data services in the specified grid areas as soon as the MO enters those areas. Additionally high *k* will be set for the obfuscation software which will *k*-anonymize the adjacent nearest N grid cells (set by the LBS server based on grid area, road network and number of users (reference of 1). The *k* will be decremented by one in subsequent next N grid cells. The algorithm will run only on one map datasheet and will be recursively implemented on other map datasheets till the user uses LBS. Each user will be identified by a thread on the LBS server. This process guarantees highest privacy which is supposed to be achieved only through no connectivity zone followed by decreasing subsequent *k* anonymities. The proposed system hence gives much better results than the latest works of *k* –NN anonymisation techniques [2].

Static and dynamic query processing: The query point(s) of the concerned MO and the nearest locations and/ or query points of other MOs will be *k* anonymised depending on previous sections settings of privacy hierarchies. The modelling of the locations, queries, range of *k* anonymisation is done in two dimensions which is proposed to be increased to three dimensions (figure 2).

Result

The presented work is an effort towards enhancement of currently available privacy protection mechanisms. This work aims to affect live databases (real-time or continuous queries) which generally involve unreliable and inefficient dynamic DBMS. The techniques presented here are an effort towards reducing the tedious DBMS handling routines and simultaneously protecting the privacy of the users of Location Based Services which involve the internetworking.

By using double protection on the client's system as well as on the servers (local, ISP and LBS), the soft procedures are reduced. Communication transceivers (MO device and server) are the actual concerned devices required to ensure fast, reliable, privacy protected usage of quality LBS. Thus, converging user's connectivity to the next level.

Figure 4 shows how the increase in the width of the grid cells in a grid area which is the precision of the grid based technique enhances the responsetime.

These graphical results reveal that the dependency of privacy protection on a single TTP server is not advisable if some procedural changes can be incorporated to protect LBS user's privacy on both client's and server's ends.

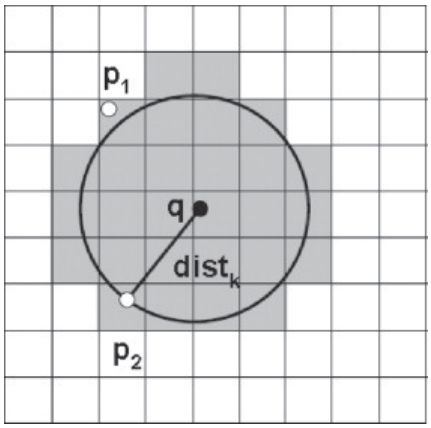

Figure 1: Example of a Grid Area on the map for obfuscation where p1 and p2 are the two subsequent positions of the MO, q is the query point. Distance for k the anonymisation can be radially found.

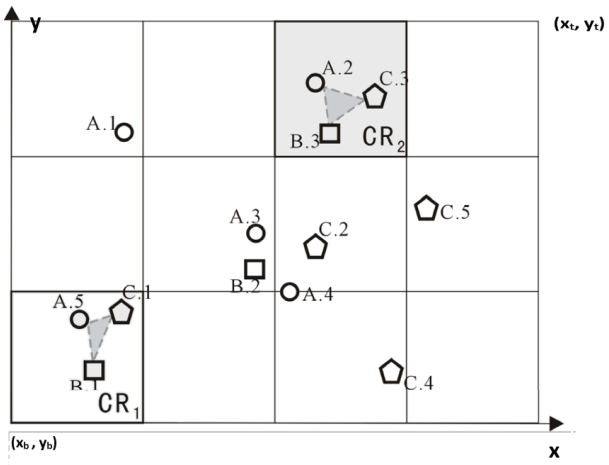

Figure 2: Co-ordinate representation of grid area showing right top corner (xt, yt) And left bottom corner (xb, yb). The current location of the MO is (xu, yu)
The defined query area is divided into n × n grid cells of equal size. Each grid cell being given by (c, r), where, c is the column number from left to right and r is the row number from bottom to top, respectively.

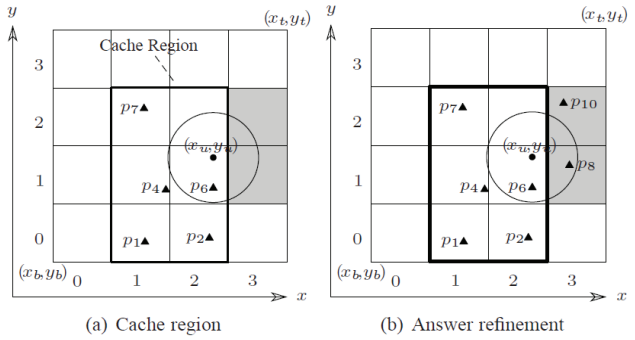

Figure 3: Example of k-NN anonymity after identification of similar grids and query answer is refined accordingly

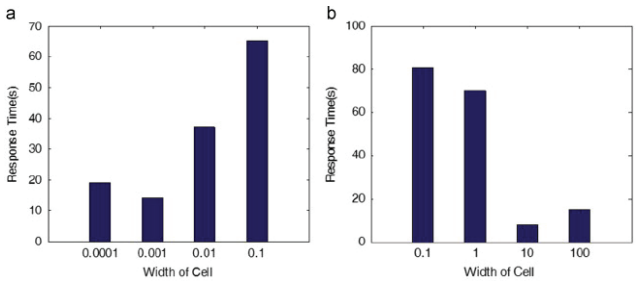

Figure 4: Query response time with respect to the width of the grid cells

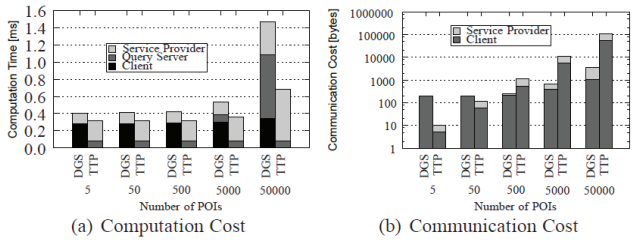

Figure 5: Comparisons of Computation and Communication costs of our proposed Direct Grid System (DGS) with the Trusted Third Party (TTP) architecture [1] in terms of number of points of interests (POI)

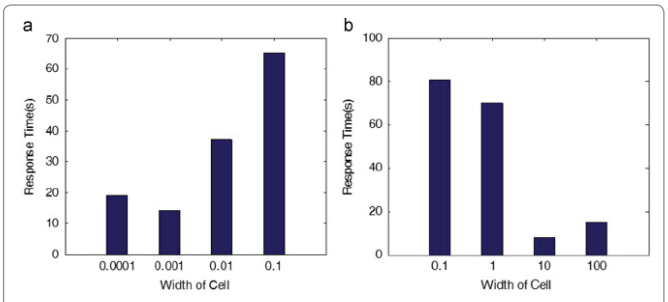

Figure 6: Comparisons of Computation and Communication costs of our proposed Direct Grid System (DGS) with the Trusted Third Party (TTP) architecture [my iete paper] in terms of number of LBS users

This work can be further improved by generating larger datasets, working with real data (as we have provided more simulation results for the lack of real data) and increasing the two dimensions of obfuscation to three dimensions or more.

References

1. Zuberi RS, Lall B, Ahmad SN. Privacy protection through k. anonymity in location. based services. IETE Technical Review. 2012;29(3):196-201.
2. Aal-Nouman M, Salman OH, Takruri-Rizk H, Hope M. A new architecture for location-based services core network to preserve user privacy. In New Trends in Information & Communications Technology Applications (NTICT), 2017 Annual Conference on IEEE. pp. 286-291.
3. Zhong S, Li L, Liu YG, Yang YR. Privacy-preserving location-based services for mobile users in wireless networks. Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297. 2004.
4. Yanagisawa Y, Kido H, Satoht T. Location Privacy of Users in Location-based Services. In Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on (pp. 1-4). IEEE. 2006.
5. Bou Abdo J, Bourgeau T, Demerjian J, Chaouchi H. Extended privacy in crowd sourced location-based services using mobile cloud computing. Mobile Information Systems. 2016;2016:1-15.
6. A Gkoulalas-Divanis, VS Verykios. A free terrain model for trajectory K-anonymity. In Proceedings of the 19th International Conference on Database and Expert Systems Applications (DEXA). 2008;49-56.
7. Aris Gkoulalas-Divanis P Kalnis, VS Verykios. Providing k-anonymity in Location based services. ACM SIGKKD Explorations Newsletter. 2010;12(1):3-10
8. MF Mokbel, CY Chow, WG Aref. The New Casper: Query Processing for Location Services without Compromising Privacy, In Proceedings of 32nd International Conference on Very Large Data Bases (VLDB 2006). 2006 Sep;pp.763–774.
9. Arain QA, Memon I, Deng Z, Memon MH, Mangi FA, Zubedi A. Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks. Multimedia Tools and Applications. 2017;1-45.
10. Zuberi RS, Ahmad SN. Secure mix-zones for privacy protection of road network location based services users. Journal of Computer Networks and Communications. 2016;2016:1-8.
11. Garcke J, Griebel M. Semi-supervised learning with sparse grids. SFB 611.
12. Bissias GD, Liberatore M, Jensen D, Levine BN. Privacy vulnerabilities in encrypted HTTP streams. In International Workshop on Privacy Enhancing Technologies. Springer, Berlin, Heidelberg.