ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Search Me If You Can Privacy-Preserving Location Query Service

Akash Mishra, Shefali Kadam, Avinash Kumar, Sharvari Shinde

Department of Computer, Dr. D Y Patil Institute of Engineering and Technology, Pune, India

ABSTRACT: Now-a-days Location-Based Service (LBS) has become increasingly popular with the dramatic evolution of smartphones and social network services (SNS). Its context-rich functionalities attract significant users. Many LBS providers use information regarding users' location to offer them convenience and beneficial functions. However, the LBS could significantly breach personal privacy because location itself contains much information. Therefore, preserving users' location information and at the same time achieving utility from applications is still a challenging task. This paper deals with non-trivial challenge by designing a collection of novel fine-grained Privacy-preserving Location Query Protocol (PLQP). The protocols designed allow different levels of location query on encrypted location information for different users and it can be applied to mobile platforms due to its high efficiency.

KEYWORDS: spatial cloaking, k-anonymity, location privacy, privacy protocol, location query, location based server.

I. INTRODUCTION

With the development in the field of smartphones, Location Based Services (LBS) have become one of the most popular applications. The smartphones furnished with the facility of GPS, have immense computational ability to access and process users' location information. This has flooded the use of LBS in smartphones. Let us take a very good example of a smartphone camera: when one clicks a photo from the camera then date, time and location is automatically attached with the picture. Additionally, the rapid growth of social network services (SNS) also helped its growth by connecting location information and social network. Similarly, there are many applications that make use of both LBS and SNS. These applications offer many attractive services but location information contains information which is much more than barely location and this could leak unwanted information.

Location Based Service (LBS) provide a wide range of services to mobile users that have been proven effective through many commercial products and research archetypes. These services include transportation services, convenience services, emergency control etc. Location Based Service (LBS) providers need users' exact location to answer their location based queries, e.g. range and nearest neighbour queries. The probability of privacy risk increases if server is potentially unwanted service provider.

In the recent times, spatial cloaking technique is used in order to preserve user privacy. The basic idea behind spatial cloaking is to map exact location of the user into cloaked area in such a way that cloaked area satisfies user stated privacy requirement. This can be done by deploying a third trustworthy party which is known as Location Anonymizing Server (LAS). This server act as a mediator between users and LBS database servers. The most important privacy requirement for spatial cloaking technique is K-anonymity, i.e., a cloaked area contains at least K users and minimum area A*min*, i.e., the size of a cloaked area is minimum A*min*. The LAS gathers users' location information and maps it into a cloaked region which satisfy the user's privacy requirements, such as *k-anonymity* i.e. user cannot be identified from the other *k*-1 users, or the minimum cloaked region area, denoted as *Amin* i.e. user needs to hide inside a region at least of size *Amin*. Since a location-based database server do not know about the user's exact location information, so the database server can only return an answer set that includes the exact answer to the user.

II. RELATED WORK

Hua Lu , Christian S. Jensen and Man Lung Yiu [1] suggested the PAD approach that is capable of offering privacy-region assurances. To do this, PAD uses so-called dummy locations that are intentionally generated according to either

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

a virtual grid or circle. These cover a user's definite location, and their spatial extents are measured by the generation algorithms. The PAD approach only needs a lightweight server-side front-end in order for it to be combined into an existing client/server mobile service system. In addition, query results are ordered according to a compact format on the server, which not only cuts communication cost, but also enables the result refinement on the client side. An experiential study shows that proposal is effective in terms of offering location secrecy, and proficient in terms of computation and communication costs.

Po-Yi Li ,Wen-ChihPeng, Tsung-Wei Wang, Wei-Shinn Ku, Jianliang Xu and J. A. Hamilton, Jr. [2] proposed a cloaking algorithm in which cloaked regions are produced according to the features of spatial networks. By exploring the properties of spatial networks, the cloaked regions are very effective for reducing query results and enhancing cache utilization of mobile devices. Moreover, an index structure for spatial networks is made and in light of the proposed index structure, we generate a Spatial-Temporal Connective Cloaking algorithm (STCC). A simulator is implemented and widespread experiments are conducted. Experimental results show that projected algorithm outstrips prior cloaking algorithms in terms of the candidate.

Bugra Gedik and Ling Liu [3] described a scalable architecture for guarding the location privacy from numerous privacy threats resulting from uncontrolled usage of LBSs. This architecture consist of the development of a personalized location anonymization model and a group of location perturbation algorithms. A unique property of our location privacy architecture is the use of a flexible privacy personalization structure to support location k-anonymity for aextensive range of mobile clients with context-sensitive privacy requests. This framework allows each mobile client to state the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to receive when requesting k-anonymity-preserving LBSs. The personalized location k-anonymity model, together with users' location perturbation engine, can accomplish high resilience to location privacy intimidations without introducing any substantial performance penalty.

Yu Wang, Dingbang Xu, Xiao He, Chao Zhang, Fan Li and Bin Xu [4] introduced a new location privacy problem: Location-aware Location Privacy Protection (L2P2) problem, where users can express dynamic and diverse privacy requirements for different locations. The objective of the L2P2 problem is to find the smallest cloaking area for every location request such that diverse privacy requirements over spatial and/or temporal dimensions are fulfilled for each user. They formalized two versions of the L2P2 problem, and proposed several efficient heuristics to provide such location-aware location privacy protection for mobile users. With the help of multiple simulations on a large data set of trajectories for one thousand mobile users, we approve the effectiveness and efficiency of the proposed L2P2 algorithms.

Kar Way Tan, Yimin Lin and Kyriakos Mouratidis [5] introduced the theory of information leakage in spatial cloaking. They provided methods of this leakage, and showed how they can use it for better performance in a tunable manner. The proposed approach directly applies to centralized and decentralized cloaking models, and is freely deployable on existing systems.

III. COMPARATIVE STUDY

Paper No	Author and Year	Observation	Remark
1	Hua Lu , Christian S. Jensen and Man Lung Yiu in the year 2008	Focus on three performance aspects: privacy area, communication cost, and server module cost.	Projected PAD, a privacy-area aware, dummy based location privacy protection method for mobile services.
2	Po-Yi Li , Wen-Chih Peng, Tsung-	A spatial network is distributed into grids and a pyramid data structure is implemented.	Projected a cloaking algorithm in which cloaked regions are produced

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

	Wei Wang, Wei-Shinn Ku, Jianliang Xu and J. A. Hamilton, Jr. in the year 2008		according to the features of spatial networks.
3	Bugra Gedik and Ling Liu in the year 2008	Job of a location anonymity server is to convert each message received from mobile clients into new message that can be safely (k-anonymity) advanced to the LBS provider	Projected a personalized k-anonymity model for providing location privacy.

Paper No	**Author and Year**	**Observation**	**Remark**
4	Yu Wang, DingbangXu, Xiao He, Chao Zhang, Fan Li and Bin Xu in the year 2012	Privacy requirements of user are dynamic and not static.	L2P2 allow mobile users to define dynamic and diverse privacy requirements.
5	Kar Way Tan, Yimin Lin and KyriakosMouratidis in the year 2009	Information leakage requirements have always existed in spatial anonymity approaches, but have never been identified and treated independently	Described meaningful leakage measures and proposed a methodology to control it.

IV. PROPOSED FRAMEWORK

We will develop a mobile based application for searching query and hiding users' location. The framework for the application consists of following modules:

A. Registration

In this module, we will develop a database for new user. The database contains various fields for the user viz name, pin, email id, mobile. By filling this information the user registers for the app and can login into it.

B. Login

Every registered user is assigned a unique username and password. Using this username and password the user can login into the application and retrieve utility.

C. Current location

After successful login of the user , the current location of the user is displayed on the map.

D. Select Peer

According to the current location of the user, the anonymous users in the vicinity of the user are generated. The anonymous user which is nearest to the user is selected to forward the query to location based server. In this way location of actual user is hidden.

E. Searching and cloaking

The query fired by the user is sent to the server. The server resolves the query and send it back to the user in the form of result set. The location of the user is hidden from server as query is forwarded to the server via anonymous user.

F. Display map

The result of the query is in the form of map. According to the query of the user, the server displays the map in return to the query.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V.CONCLUSION

We projected a fine-grained Privacy-preservingLocation Query Protocol (PLQP), which successfully solvesthe privacy issues in prevailing LBS applications and providesnumerous location based queries. The PLQP uses noveldistance computation and comparison protocol in order to implementsemi-functional encryption that supports multi-levelled accesscontrol. Also,during the whole protocol, until intended by the locationpublisher, the location information of the user is kept secret to anyoneelse. We also conducted experiments to show thatthe performance of our protocol is applicable in a real mobilenetwork.

REFERENCES

[1] Hua Lu , Christian S. Jensen and Man Lung Yiu proposed "PAD: Privacy-Area Aware Dummy Based Location Privacy for Mobile Services" in the year 2008 ACM 978-1-60558-221-4
[2] Po-Yi Li , Wen-ChihPeng, Tsung-Wei Wang, Wei-Shinn Ku, JianliangXuand J. A. Hamilton, Jr. proposed "A Cloaking Algorithm based on Spatial Networks for Location Privacy" in the year 2008 IEEE DOI 10.1109/SUTC.2008.56
[3] B.Gedik and Ling Liusuggested"Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms" in JANUARY 2008 IEEE TRANSACTIONS ON MOBILE COMPUTING.
[4] Yu Wang, DingbangXu, Xiao He, Chao Zhang, Fan Li and Bin Xu proposed "L2P2: Location-aware Location Privacy Protection for Location-based Services" in the year 2012 Proceeding IEEE Infocom
[5] Kar Way Tan, Yimin Lin and KyriakosMouratidis proposed "Spatial Cloaking Revisited: Distinguishing Information Leakage from Anonymity" in the year 2009 *Research Collection School of Information Systems (Open Access).* Paper 880