Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.149 – 153

REVIEW ARTICLE

REVIEW ON EXPLOITING SERVICE SIMILARITY FOR PRIVACY IN LOCATION BASED SEARCH QUERIES

Nandini K[1], Prof. Gangadhar Immadi[2]

[1]M.Tech (Software Engineering), New Horizon College of Engineering, Bangalore, India

[2]Assistant Professor, Department of Information Science & Engineering, New Horizon College of Engineering, Bangalore, India

[1] Nandini.kulkarni1990@gmail.com; [2] Immadi.gangadhar@gmail.com

Abstract: The search for nearby Points-Of-Interest (POI) has greatly improved by the introduction of global positioning systems in smart phones. This technological innovation allows any application developer to provide the geographic location of the user. Location-Based Services (LBS) utilize the positioning capabilities of a mobile device to determine the current location of a user but it's this application lack behind in the privacy controls to user information without affecting the usability of the services. This paper explains about various frameworks to provide privacy to the individual information along with satisfied services from the service provider. The integration of the LBS architecture along with the Geo-coordinates. In this paper we explain the various architecture and demonstrate the secured user privacy.

Keywords: Location Based Services (LBS), Privacy-supportive, location privacy, service quality.

I. INTRODUCTION

The current rapid increasing use of smart phones, the mobile location based service market is growing to the point that location-based services are now a standard feature on many mobile devices. Contribution to the rapid growth of location tool is due to the greater availability of GPS phones, reduced prices, and app stores For example, with the iPhone 3G now priced at $99 (with service agreement), GPS-enabled phones are within the reach of many consumers.

A Location-Based Service (LBS) is a mobile computing application that provides services to users based on their geographical location. The common questions can raise in LBSs are "Tell where the nearest coffee shop is ?", "Give the location of the ATM within 5 km range ?".

"Privacy" and "Usability" are requirement of successful of Location based application. Privacy (location) is loosely defined as a personally assessed restriction on when and where someone's position is deemed appropriate for disclosure. Usability has a twofold meaning

- Privacy controls should be intuitive yet flexible, and
- The intended purpose of an application is reasonably maintained.

With the rapid growth of new technologically innovative application, there also growth in the challenges faced by the researchers. The major challenge in LBS is the abuse of mobile user's location data, which gives raise in the lack of preserving the user private personal information.

This survey paper aims to provide an overview of the different architectures, methods and the new technologies in which the LBSs are based. The paper is organized as follows. Section II describes the various ways of attack can take in to access the user location and the user's information. Section III presents the architecture, frameworks and the different ways to secure the location information of a individual user and lastly, Section IV concludes the survey with a summary of the related researches and an overview of current and future related research.

II. CLASSIFICATION OF LOCATION PRIVACY ATTACKS

The variety of possible attacks, which will become a challenge to protect the privacy of location information. The attacks on the privacy of user profile can be differentiated in the following different attacks [1]:

1. ***Single position attack:***
In the single position attack, the attackers analyze the single request or the query or the updates of the user to collect more information about the location and the profile that the user is hiding.

2. ***Context linking attack:***
In this approach, attacker use personal context knowledge to reduce the user privacy. The attacker exploits Context information in addition with the external environment of the user such as a map etc. Context linking attack can be distinguished between three different kinds of attack:

- Personal context linking attack: knowledge about the individual user's personal profile.
- Probability distribution attack: based on collection of the traffic statistics and environmental context information.
- Map matching: based to restrict the obfuscation area from where the attacker can analyze the user location.

3. ***Combination of multiple position and context linking attack*****:**
An attacker can also combine several of the proposed attacks or use them in sequence to undermine the user's location privacy.

4. ***Compromised trusted third party:***
In compromised trusted third party (TTP), as the name, the attack take place through the third party system where the information is stored or collected. The attack on a TTP is realistic and not negligible. Thus, it is to be worried to assume the trustworthiness on the third party.

III. DIFFERENT METHODS AND TECHNOLOGY FOR THE LOCATION PRIVACY

A . ***Location Privacy***

In this framework [2], system model that connects privacy, service quality and cloaked information is described. This model describes the privacy of the user requirement. Figure 1 illustrates [2], In this idea is to allow the user to specify location and privacy requirements to the cloaking agent. Then the cloaked location (i.e., a larger region that contains the user s true location) and an "imprecise" service request is built in the service provider. On collected 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 other system. In Figure 1 it can be seen that a user can first specify its privacy preferences through a privacy language.

Privacy language, that is generated, is allowed to specify privacy preferences with respect to:

i. *Locations*: Locations can be logical or physical. Cloaking is required when the user is near to a specific required object;

ii. *Service providers and other users*: the location of the user may also be made known (or hidden) to specific users and service providers.

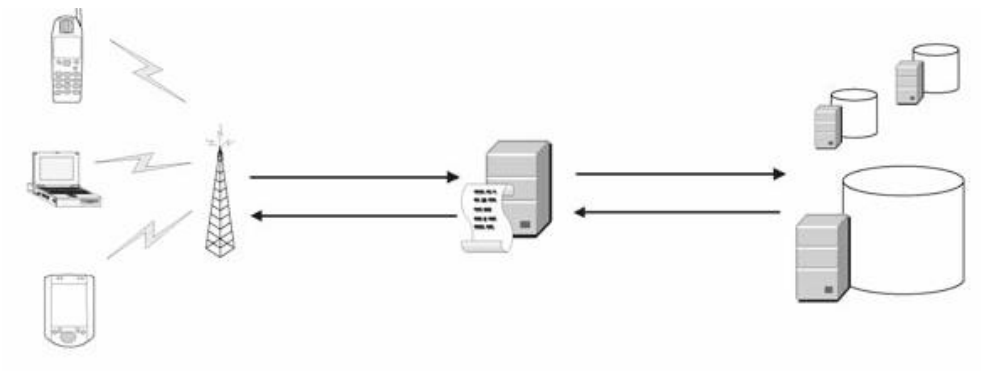

Fig.1 Managing Privacy and Service Quality with the Cloaking Agent

Inside the cloaking agent, the user s privacy preferences are then sent to the policy translator. The policy translator produces a cloaked location based on the precise location sent by the user and requirements. For instance, if the user s requirement is generate a cloaked location that covers five buildings, when I am in Area "X", the policy translator produces the corresponding cloaked location, when it detects the user is in Area X. The policy translator is also sent 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 is processed by the cloaked data. Based on the cloaking agent, the user can then decide if the degree of privacy should be reduced. A novel architecture for LBS applications that is directed toward revealing privacy/utility tradeoffs to a user before an actual geo-tagged query is made. Unlike other architectures 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 [1].

B. ***Position dummies***

In [3] anonymous communication technique is to protect the location and the personal information of the LBS user. In this technique, the user sends his/her true or the extract location information among the false location data ("dummies") to the service provider. Once the reply is obtained from the service provider, the user will extract the necessary information from the obtained reply. In this technique, if at all the service provider stores the user location information, the attacker cannot distinguish the true location of the user among the set of false location information. The technique should applied by keeping in mind about the following two issues:

i. Realistic dummy movements
ii. Reduction of communication costs

C. ***Anonymous Location***

Traditional encryption methods aim at providing "unbreakable data", which means that the way to deal with security threats is to apply encryption on the plain data and to allow only authorized parties to perform decryption. The encryption technique in LBS is divided in two methodologies; the first one focuses on encrypting the user location to achieve provable location privacy [4], [5]. The endeavour of this technique is to prevent the attacker from obtaining user's data, where this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. Li and Jung [6] designed a fine-grained Privacy-preserving Location Query Protocol (PLQP). Their protocol allows different levels of location query on encrypted location information for different users. Wong et al. overcame this drawback by developing an asymmetric scalar-product preserving encryption [7]. This allows the preservation of relative distances between database points.

X. Sean Wang, and Sushil Jajodia [8] discussed the ideas about algorithms to prevent the privacy issues involved in the location-based services. It is investigated that, if the user identity is not explicitly given to the service provider, but the Geo-localized history of user-requests can act as quasi-identifier(set of attribute, that is stored in database, as a user personal information) and can be able to access personal information about the users. Thus, this paper describes the risk in revealing the user identity and information.

D. *K-anonymity without Cloaked Region*

In a new framework called K-anonymity Without Cloaked Region (KAWCR) to protect privacy in location information. KAWCR can guarantee that the user issuing the query is indistinguishable from at least K-1 other users. Compared with K-anonymity, KAWCR needs INN query processing algorithm while K-anonymity needs complex processing algorithm at the server side, and the cost of communication in KAWCR is lower than that of K-anonymity on some datasets. Compared with SpaceTwist, the KAWCR and SpaceTwist needs INN query processing algorithm at the server side, but the cost of communication of KAWCR is lower than that of SpaceTwist on some datasets, when they provide the same level of privacy. TABLE I summarizes the three techniques proposed in this paper [9].

TABLE I . THREE TECHNIQUES

	KAWCR TRADITION	***K*-ANONYMITY**	**SPACETWIST**
K-anonymity	Yes	Yes	No
Query processing cost	Low	High	Low
Communication cost	Low	High	High

E. *LBS architectures*

T. Tsiligiridis, C. Pontikakos and T. Glezakos[10] describes about the various location based services systems and it will focuses on their architectures and the platforms and the related technologies on which the services are based. The description is started with the first level of classification on the positioning infrastructure like indoor, network based. LBS architecture is classified based on the functionality and the various characteristics based design. The author future discussed about the integration of the LBS and the different geographical information system (GIS).In order to grow the interoperability among the various systems and the related technology, the needed standardization and homogenization is taken under consideration.

F. *Obfuscation and coordinate transformation*

M. Duckham and L. Kulik [11] describes about framework within which obfuscate location based services are defined and provides efficient mechanism for high quality information against the user location privacy. Author described about the negotiation mechanism to ensure that a service provider receives only the required information that help to provide service of satisfied quality. Issues approached in this paper is, the protecting sensitive information about an individual user's location with providing the satisfied information to the user.The user location privacy is obtained by deliberately degrading the user information and this process is known as obfuscation. The main aim of this paper to develop:

i. A general model of obfuscation.

ii. An algorithm for computation of general obfuscated location based services.

iii. A procedure for achieving negotiation between an individual and a service provider.

iv.

IV. ISSUES IN LOCATION PRIVACY

The various methods and the technology discussed in section II, arises following issues.

i. the location information will be among the result set, which makes the attacker to know about the individual user information.

ii. Location cloaker system is not secure, the unknown person can alter the user information or miss use the information.

iii. In Negotiation model, the user need to mention his/her location information as in the query to the service provider.

V. CONCLUSION

This review illustrates the overview on what works have been conducted regarding location based services. The various areas of the LBSs, including privacy, point of interest, performance of the service etc. are presented .The discussed the various methods and techniques to determining the user privacy in LBS and to provide the service object that are needed by users to be in the near location.

REFERENCES

[1] M. Wernke, P. Skvortsov, F. Durr and K. Rothermel, *A classification of location privacy attacks and approaches*,Parallel and Distributed Systems, IEEE Transactions, vol. 20, no. 4, pp. 512 - 527 , 2009 .

[2] Wei-Shinn Ku, Yu Chen, Roger Zimmermann, *Privacy Protected Spatial Query Processing for Advanced Location Based Services*, journal, vol 3, No 6, 2011.

[3] 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.

[4] G. Zhong, I. Goldberg and U. Hengartner, *Louis Lester and Pierre: Three Protocols for Location Privacy*, the Natural Sciences and Engineering Research, Canada, 2007.

[5] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg and D. Boneh, *Location Privacy via Private Proximity Testing*, in Network Distributed System Security, 2011.

[6] X.-Y. Li and T. Jung, *Search Me If You Can: Privacy-preserving Location Query Service*, in INFOCOM, Proceedings IEEE, Turin, 2013.

[7] W. Wong, D. Cheung, B. Kao and N. Mamoulis, *Secure kNN Computation on Encrypted Databases*, in the 35th SIGMOD International Conference on Management of Data, Rhode Island, USA, June 29–July 2, 2009.

[8] Bettini C, Wang X, Jajodia S (2005) *Protecting privacy against location-based personal identification. In*: Jonker W, Petkovic M(eds) Secure data management, lecture notes in computer science,vol 3674. Springer, Berlin, pp 185–199.

[9] Zhenqiang Gong , Guang-Zhong Sun, Xing Xie , *Protecting Privacy in Location-based Services Using K-anonymity without Cloaked Region*, in china, Eleventh International Conference on Mobile Data Management

[10] T. Tsiligiridis, C. Pontikakos and T. Glezakos, *Location-based services: architecture overview*, in ITAFE, Turkey, 2005.

[11] M. Duckham and L. Kulik, *A Formal Model of Obfuscation and Negotiation for Location Privacy*, in Third Int'l Conf. Pervasive Computing, Berlin, 2005.

