Cloud Publications
International Journal of Advanced Remote Sensing and GIS
2013, Volume 2, Issue 1, pp. 398-404, Article ID Tech-171
ISSN 2320 - 0243

Review Article **Open Access**

Location Privacy in Location Based Services: Unsolved Problem and Challenge

Rajchandar Padmanaban

Institute for Geoinformatics, University of Muenster, Germany

Correspondence should be addressed to Rajchandar Padmanaban, Charaj7@gmail.com

Publication Date: 9 December 2013

Article Link: http://technical.cloud-journals.com/index.php/IJARSG/article/view/Tech-171

Abstract Location Based Services (LBS) is one of the emerging technologies in the mobile, networking and information services. LBS, the branch of computer program-level services used in various fields and support, the application are broadly classified as Maps and Navigation, Information service, Tracking service, Games, Social networking, Vehicular navigation and Advertising. Location is mainly determined into two levels such as internally by a device or externally by systems and kind of networks with which the device interrelates. The advanced mobile networking and communication lend a hand to the civilization with various location based mobile application but while concerning about location privacy, there is most prominent question from the society, how about my location privacy? This article reviews a selected level of privacy in location based services that have been published in the different research journal. The review throws light on the threat and remedy on location privacy in the location based application and services that are represented.

Keywords *Location-Based Service; Location Privacy; Security, Threats; Computational System*

1. Introduction

By tradition, mobile networks utilized customer location for data transmission and voice broadcast but recent days the user location extensively employed for Location Based Services. Secrecy is the most considered factor for the people and is the most important feature the developers to keep in mind while developing the applications. Over the last few decades many research focus on the location privacy but still contradiction and challenges in conquer these risk. The techniques and methodology varied according to the application of location based service.

The major component of location privacy differentiates according to the information processing and temporal sequence. These activities are including, (1) collection of data; (2) retention or improper storage; (3) use of data; (4) revelation of location associated information. Some of the suggested techniques used in the last few decades to overcome the location privacy threats such as spatial k-anonymity, dummy location, cloaking/obfuscation, cryptographic, Trusted third party protocol (TTP), simple and multiple pseudonym, semi distributed protocol, Private Information Retrieval protocol (PIR), collaborative protocol, and user centric and so on. This paper is structured in three sections. The first section focuses the review of literature in the branch of location privacy. The second section describes the location privacy threats, how they are affecting the individual. The third section illustrates the various techniques used in the location privacy in the last few years in the research community; what are all the frequent and contradiction among the techniques. The last section focus on the present and future thought about the location privacy in location based service.

2. Literature Review

In generally threats can be classified into two types they are communication privacy threats and location privacy threats [1]. MarcoGruteser and Dirk Grunwald ponder on sender anonymity on communication privacy threats. Anonymity in LBSs must be addressed at multiple levels in the network stack depending on what entities can be trusted [1]. In matching approach, Bugra Gedik and Ling Liu develop a spatio-temporal cloaking model, called Clique-Cloak algorithms, its aid to offer high quality location privacy k-anonymity model, development at avoiding position privacy threats before handoff the request to location based service provider [2].

In addition, Obfuscation model used in the pervasive computing environment. Obfuscation, framework, negotiation is employed to make sure that a location-based service supplier receives only the information which is need to provide a service [3].

Mohamed F. Mokbel *et al.,* developed a system called Casper; it encloses two mechanisms, including: Location anonymizer and privacy-aware query processor. The privacy-aware query processor is installed inside the LBS database server to facilities cloaked spatial area rather than the precise position of the mobile user’s [4]. In related to that various set of Location based Quasi-identifiers as spatio-temporal patterns suggested by Claudio Bettini *et al*.

In research, mix zone model proposed by Alastair R. Beresford and Frank Stajano, the plan of the mix zone is to stop tracking of long-term mobile user’s activities, but still permit the operation of many short-term location-aware applications [6]. The location privacy can be achieved by nearest neighbourhood analyses likewise space Twist technique developed by Man LingYiu *et al.,* rectifies these inadequacy for k nearest neighbour (kNN) queries. Starting with a position dissimilar from the user’s actual location, nearest neighbours are retrieved incrementally until the query is answered correctly by the mobile terminal [7].

In the sequence of suggestion, dummies also used for avoiding threats in location privacy, this system personal user of a location-based service generates several false position data (dummies) sent to the service provider with the true position data of the user [8].

Diversely Location privacy based on a homomorphism developed by Solanas Agusti and Antoni Martínez-Ballesté, homomorphism as a tool for processing mobile network communication data with the assist of encryption and decryption function. Likely, Cryptographic is the prominent tool used in the communication data conversion for avoiding risk from location privacy. One of the application from cryptographic called blind signature it was proposed by Qi He, Carnegie Mellon University, which is used to produce a certified anonymous ID that restore the real ID of an authorized mobile communication device [10].

Lothar Fritsch and Tobias Scherner suggested a middleware system to control the flow of information and to guard the interest of every party. This system comprised of three components such as matcher, identity management system and process control. Privacy mechanism also based on different service component, including: (1) LBS service component; (2) Localization component; and (3) communications component [13].

Protecting privacy in vehicular service is also one of the great deal while concerning location privacy, the Vpriv is the vehicular based location privacy application fashioned by Raulca ada papa *et al.,* this system the cryptographically produced random tags are used for the registration to avoid location stealing. In different way location privacy in vehicular network can protect through Path Confusion method. The path perturbation algorithm developed by Baik Hoh and Marco Gruteser at WINLAB, The key idea in this algorithm based on cross path in area where at least two or more users meet at same time and confuse the path of different users [15].

A Privacy-Preserving Location proof Updating System (APPLAUS) fashioned by Zhichao Zhu and Guohong Cao, the main key factor of this system capable of generating different Periodical pseudonyms are used by the mobile devices in order to protect the mobile users location privacy from each other, and from the un- trusted location proof mobile communication server [16].

3. Location Privacy Invading

Location information of mobile user’s been collected and employ, knowingly or unknowingly; the geographic location of mobile user can easily expose in the location based service application. Knowing where is the customer, what he is doing: attending any meeting or event, spending time in the bar, visiting a doctor, taking public transport and so on. The location information assist to analyse the individual interest of consumer, which place mostly visited by consumer: information used for advertising and marketing. When Location data combined it reveal consumer regular habits and everyday work: how often in that particular place, what is the individual interest, whom and how he spends time. Location based service also make easy to collect information about customers / users such as name, age, sex, friends or relatives details and so on, individual information also steals by someone for their personal interest.

3.1. Location Privacy Threat in Geo-Tagging

Geo-tagging is also direct to threats in location privacy, modern device like iphone, smart phone, digital camera and video camera enclose geo-tagging option, while enabling geo-tagging option in the device its automatically tag the geolocation of the user in the picture, while uploading these pictures in the social network such as YouTube, Facebook, twitter, Google + and Flickr may leads to invading of personal interest and location with the scrutinize of metadata in the server / database.

4. Techniques Involved in the Location Privacy

Anonymity is the prominent model for providing trustable location based application to the society. This system carries connection between the mobile nodes and anonymity server, initially the encryption process carried out in the anonymity server, during the communication between mobile nodes and server, the position and other information will decrypts at anonymity server and its remove other information like address of the network and position data. In same way several algorithm proposed in the literature [1, 2] but recent research says that these techniques refers to spatio anonymization problem. As briefly the idea of the spatio anonymization problem is that user of the location based application can be identified through their position / location, and consequently user’s privacy become endangered if a widespread request holds precise information about mobile user’s location.

Existing approaches to the spatio anonymization problem [1, 17, 18] propose techniques that are secure also in the case in which the attacker obtains the precise location information of every mobile user. Even though various research overcome the anonymity problem still we need the appropriate framework to model for privacy attack based on the multiple requests.

To protect the micro data in the server can accomplish by K Anonymity technique K anonymity mainly helps to preserve the truthfulness of the user's information. Multilevel databases used in the k anonymity techniques, the different level arrangement has facilitate to store the data at different security classification and also user's holding dissimilar security authorization but unfeasible to consider every possible attack. In other concern numerous holder share same data and repression reduce the quality of the data so feasible approach need to overcome the disadvantage of K anonymity.

In order to overcome the traceable problem in Location Based Services, a new type of anonyms technique proposed in the literature [8] is Dummies location. It sends the position of the user information including noise to the service provider. The noise consists of false location of the user's called dummies. Hidetoshi Kido *et al*., proposed the dummy generation algorithm with two set of models are Moving in Neighborhood and Moving in a Limited Neighborhood accomplished in different external server but another approach proposed in the literature [20] focusing on the Circle-Based dummy generation and Grid-Based dummies generation algorithm requires lightweight server-side front-end to integrate the existing mobile network system.

Potentially, three set of limitation can observe in the spatial information while using assorted location privacy models they are imprecision, ambiguity and inaccuracy. Obfuscation [3] also degrading the superiority of information about an individual position in order to protect that mobile user's position.

Cryptography technique also used in the research group for avoiding position traceable, it's capable of sharing information with high security, data integrity in several database and intense authentication in mobile network. In privacy model cryptography served in both online and offline trusted third party. Trusted third party schema mostly based on spatial K- anonymity and cloaking/obfuscation for protecting the association between user identity and location. Hilbert based algorithm [24] and Icliqueclock [25] are the recent research focused on providing better model to overcome the various disadvantage faced in the location privacy frame work, the main difference between these two algorithm are Hilbert is based on the geographic related algorithm and icliquecloak related on the geometry based algorithm, icliquecloak clearly its adapted from the K anonymity and cloaking algorithm. The Table 1 shows the various models of location privacy system and its pros and cons proposed by literatures in last ten years.

Table 1: *Various Models / Framework of Location Privacy*

Models / Framework	Advantage	Disadvantage	Academic Literature
Simple Pseudonym	Identity privacy	Low accuracy Unlink ability	Hauser, Christian, and Matthias Kabatnik, 2001
K anonymity	Location Privacy	No identity privacy Unlink ability	Gruteser Marco & Dirk Grunwald, 2003 Gedik, Bugra, and Ling Liu,2005 Bettini, Claudio, X. Sean Wang, and Sushil Jajodia, 2005
Mixzone	Location and sampling accuracy	Operation Lack in multiple responder	Beresford, Alastair R., and Frank Stajano, 2004
Obfuscation	High server efficiency Location privacy	No identity privacy Unlink ability	Duckham, Matt, and Lars Kulik, 2005
False Position Data/ Dummies	Easy to integrate with existing mobile network	Operation Lack in multiple responder	Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh, 2005
Location Anonymizer – Cloaking Algorithm	Accuracy, Flexibility	Unlink ability	Mokbel, Mohamed F., Chi-Yin Chow, and Walid G. Aref, 2006

K nearest Neighbor (kNN) Queries	No need of middleware Sever side granular search technique	Cost model	Yiu, Man Lung, et al.,2008
Trusted Third Party (TTP) - Pseudonymisation	Robust against the collusion of a Malicious user	Not centralized	Solanas, Agusti, and Antoni Martínez-Ballesté, 2008
Cryptographic	Automated	High cost	Popa, Raluca A., Hari Balakrishnan, and Andrew J. Blumberg,2009
Private Information Retrieval (PIR) Protocol	Location privacy	Low LBS server efficiency	Ghinita, Gabriel, 2009
ICliqueCloak	Many responders	Possibility of attack	Pan, Xiao, Jianliang Xu, and Xiaofeng Meng. 2012
Hilbert Based	Quick query processing time Location privacy	High cost	To, Quoc Cuong, Tran Khanh Dang, and Josef Küng, 2013

5. Conclusion

Current research focuses on the location user privacy and trouble-free frame work for interconnecting the mobile network and privacy model server. There are well-known model, k anonymity and cloaking algorithm used in various literatures but still we need efficient tool to handle the location privacy threats, topical framework focus on the geographic based algorithm instead of geometry based algorithm. As literally review shows system naturally need competent model to protect from unauthorized access as well as mobile user need the well-organized tool to secure their context information from illegal access. This paper surveyed various techniques used in the different approach based solutions for attaining privacy protection in the Location Based Service (LBS).

Location privacy research is still in fundamental level. Even though inventive model have been proposed to resolve the privacy problem in Location Based Service (LBS), there are many challenges faced by research group. Inventing a new structure of algorithm the various disadvantage of existing model should taken into consider. In one hand, interlinking of mobile network and secure framework still many challenges to be addressed, in another hand lack of technology in multiple responders' problem. Furthermore research also needed in location privacy, including: (1) Link ability problem; (2) Collusion of malicious user trouble; (3) Operation in multiple responder; (3) Identity privacy; (4) LBS server difficulty; and (5) Middleware network issue. We are look forward to many beneficial investigate on the difficulty in mounting location privacy system.

References

[1] Gruteser Marco and Dirk Grunwald. Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. Proceedings of the 1st International Conference on Mobile Systems, Applications and Services. ACM, 2003.

[2] Gedik Bugra and Ling Liu. Location Privacy in Mobile Systems: A Personalized Anonymization Model. Distributed Computing Systems, 2005. ICDCS 2005. Proceedings of 25th IEEE International Conference on. IEEE, 2005.

[3] Duckham Matt and Lars Kulik. *A Formal Model of Obfuscation and Negotiation for Location Privacy. Pervasive Computing.* Springer Berlin Heidelberg. 2005. 152-170.

[4] Mokbel Mohamed F., Chi-Yin Chow, and Walid G. Aref. *The New Casper: Query Processing for Location Services without Compromising Privacy*. Proceedings of the 32nd International Conference on Very Large Data Bases. VLDB Endowment, 2006.

[5] Bettini Claudio, X. Sean Wang, and Sushil Jajodia. *Protecting Privacy against Location-Based Personal Identification*. Secure Data Management. Springer Berlin Heidelberg. 2005. 185-199.

[6] Beresford Alastair R. and Frank Stajano. *Mix Zones: User Privacy in Location-Aware Services.* Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004.

[7] Yiu Man Lung, et al. Spacetwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services. Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on. IEEE, 2008.

[8] Kido Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh. *Protection of Location Privacy Using Dummies for Location-Based Services.* Data Engineering Workshops, 2005. 21st International Conference on. IEEE, 2005.

[9] Solanas, Agusti, and Antoni Martínez-Ballesté*. A TTP-Free Protocol for Location Privacy in Location-Based Services.* Computer Communications. 2008 31 (6) 1181-1191.

[10] He Qi, Dapeng Wu and Pradeep Khosla. *The Quest for Personal Control over Mobile Location Privacy.* Communications Magazine, IEEE. 2004. 42 (5) 130-136.

[11] Popa Raluca A., Hari Balakrishnan, and Andrew J. Blumberg. *VPriv: Protecting Privacy in Location-Based Vehicular Services*. USENIX Security Symposium. 2009.

[12] Fritsch Lothar and Tobias Scherner. *A Multilaterally Secure, Privacy-Friendly Location-Based Service for Disaster Management and Civil Protection*. Networking-ICN 2005. Springer Berlin Heidelberg, 2005. 1130-1137.

[13] Zhong Sheng et al. *Privacy-Preserving Location-Based Services for Mobile Users in Wireless Networks*. Yale Computer Science, Tech. Rep. YALEU/DCS/TR-1297 2004.

[14] Cheng Reynold et al. *Preserving User Location Privacy in Mobile Data Management Infrastructures.* Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2006.

[15] Hoh Baik and Marco Gruteser. *Protecting Location Privacy through Path Confusion.* Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. IEEE, 2005.

[16] Zhu Zhichao and Guohong Cao. *Applaus: A Privacy-Preserving Location Proof Updating System for Location-Based Services*. INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[17] Bettini Claudio, Sergio Mascetti and X. Sean Wang. *Privacy Protection through Anonymity in Location-Based Services.* Handbook of Database Security. Springer US. 2008. 509-530.

[18] Bettini Claudio, et al. *Anonymity in Location-Based Services: Towards a General Framework.* Mobile Data Management*,* 2007 International Conference on. IEEE, 2007.

[19] Sweeney Latanya. *K-Anonymity: A Model for Protecting Privacy*. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2002. 10 (5) 557-570.

[20] Lu Hua, Christian S. Jensen, and Man Lung Yiu. *Pad: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services*. Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access. ACM, 2008.

[21] Magkos Emmanouil. *Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey*. International Journal of Information Technologies and Systems Approach (IJITSA). 2011. 4 (2) 48-69.

[22] Hauser, Christian, and Matthias Kabatnik. 2001: *Towards Privacy Support in a Global Location Service.* Proc. of the IFIP Workshop on IP and ATM Traffic Management.

[23] Ghinita Gabriel. 2009: Private Queries and Trajectory Anonymization: a Dual Perspective on Location Privacy.

[24] To Quoc Cuong, Tran Khanh Dang, and Josef Küng. *A Hilbert–Based Framework for Preserving Privacy in Location–Based Services*. International Journal of Intelligent Information and Database Systems. 2013. 17 (2) 13-134.

[25] Pan Xiao, Jianliang Xu, and Xiaofeng Meng. *Protecting Location Privacy against Location-Dependent Attacks in Mobile Services.* Knowledge and Data Engineering, IEEE Transactions on. 2012. 24 (8) 1506-1519.