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

Privacy in Location-Based Services

Sampada Sarodaya[1], S. V. Dabhade[3]

[1]Smt. Kashibai Navale College of Engineering, Vadgoan, Pune, Maharashtra, India

[2]Professor, Smt. Kashibai Navale College of Engineering, Vadgoan, Pune, Maharashtra, India

Abstract: ***development of mobile communication, applications represents a challenge for both conceptually and technically so the basic requirements of LBS (location-based services) are numerous. Complex task is to provide user with added value to location information. Previously using Trajectory privacy-preserving framework user's location is preserved using various techniques, but the locations of users' trajectories may not sensitive all the time. Even mix-zones are regions where users' movement cannot be track by any applications. In this paper mobile users will reveal their location to database services in a periodic or on-demand manner. New spatial cloaking techniques based on real or historical user trajectory is designed to protect user location trajectories and also satisfy the users' specified k-anonymity level.***

Keywords: Location-based services, spatial cloaking, k-anonymity, mix-zones, mobile communication

1. Introduction

Utilizing the underlying network based on user's current locations mobile applications are useful foe tracking user's movement and deliver information. location-based services means developments of mobile devices which have flourished mobile services based on user locations. Privacy problems arise throughout the method of aggregation, storing and sharing of users location information edges mobiles user's considerably due to LBS[3]. Locations-Based Services buyed by users World Health Organization might not understand the extent to that their location information is discovered or with whom the service suppliers area unit sharing information. User will not mind others discovering his/her current location while using LSB at looking plaza to look out close restaurants. However, if once user may be a well-known famous person privacy becomes necessary once user enters a special hospital and not willing to share information with anyone else. In previous work[7] even if pseudonyms rather than true identities are unit normally want to cover up the placement trace files found names protected trajectories area unit susceptible from inferential attacker those are the register will discover true identities of the many users associated what is more to get an extended area.

In mobile networking environments location privacy protection is very difficult due to two major reason. First, in mobile network area unit sample wireless communication to intercept for example at sure public place associate listener will collect transmitted information of mobile user. As a result, partial mechanical phenomenon information related to a user's true identity is exposed to the listener. Privacy-Enhancing Technologies(PET) prohibit the restricted resources of mobile devices greatly that one might apply and deploy within the network. Consequently, instead of advanced crypto graphical technologies normally utilized in wired network current PET solutions rest on straight forward schemes to cover actually identity of mobile user from a passive register[4]. Examples are native business, social networking, route finder application, e-marketing. Photo and continues LBS are mainly two varieties of LBS. A mobile user has to report its current locations for photo LBS to a provider for desired data. To get desired continuous LBS a mobile user has to report its location to a service provider in a periodic or on-demand manner. Continuous is tougher than photo LBS in concern of privacy so adversaries sometime use spatial and temporal correlation within the user location to infer the data.

2. Background and Related Work

2.1 Dummy-Based Location

Privacy protection techniques that use k-anonymity convert an original query into an anonymous query that contains the locations of multiple users. Such techniques, however, generally fail in offering guaranteed large privacy regions at reasonable query processing costs. The PAD approach is capable of offering privacy-region guarantees. To achieve this, PAD uses so-called dummy locations that are deliberately generated according to either a virtual grid or circle [7]. These cover a user's actual location, and their spatial extents are controlled by the generation algorithms. The PAD approach only requires a lightweight server-side front-end in order for it to be integrated into an existing client/server mobile service system[2]. In addition, query results are organized according to a compact format on the server, which not only reduces communication cost, but also facilitates the result refinement on the client side.

2.2 Trajectory Privacy

The ubiquity of mobile devices with global positioning functionality such as GPS and AGPS and Internet connectivity such as 3G and Wi-Fi has resulted in widespread development of location-based services (LBS)[4]. Although LBS provide valuable services for mobile users, revealing their private locations to potentially untrusted LBS service providers pose privacy concerns. On the other hand, a mobile user has to report its location to a service provider in a periodic or on-demand manner to obtain its desired continuous LBS.

2.3 K-anonymity

Consider a data holder, such as a hospital or a bank that has a privately held collection of person-specific, field structured data. Suppose the data holder wants to share a version of the data with researchers. How can a data holder release a version of its private data with scientific guarantees that the individuals who are the subjects of the data cannot be re-identified while the data remain practically useful? The solution provided includes a formal protection model named *k*-anonymity and a set of accompanying policies for deployment. A release provides *k*-anonymity protection if the information for each person contained in the release cannot be distinguished from at least *k*-1 individuals whose information also appears in the release. This paper also examines re-identification attacks that can be realized on releases that adhere to *k* anonymity unless accompanying policies are respected.

2.4 Obfuscation

Obfuscation concerns with the practice of deliberately degrading the quality of information in some way, so as to protect the privacy of the individual to whom that information refers. Obfuscation is an important technique for protecting an individual's location privacy within a pervasive computing environment. A formal framework within which obfuscated location-based services are defined are studied. This framework provides a computationally efficient mechanism for balancing an individual's need for high-quality information services against that individual's need for location privacy. Negotiation is used to ensure that a location-based service provider receives only the information it needs to know in order to provide a service of satisfactory quality.

3. Proposed System

In this paper a new framework is created, which protect the trajectory privacy in LBS. Mobile users have to reveal their locations to database servers in a periodic or on-demand manner to obtain continuous LBS. Simply applying a snapshot spatial cloaking technique to each user location independently cannot ensure k-anonymity for a user location trajectory. Thus, new spatial cloaking techniques based on either real-time or historical user trajectories are designed to protect user location trajectories. Similar to snapshot spatial cloaking techniques, a fully-trusted third party, usually termed location anonymizer, is placed between mobile users and database servers. The location anonymizer is responsible for collecting users' locations and blurring their locations into cloaked spatial regions that satisfy the user-specified k-anonymity level and/or minimum spatial region area.

Advantages of Proposed System:
1. It improves the user's locations privacy.
2. It increases efficiency.
3. It decreases privacy loss.

4. Proposed Architecture

The factor of participators' privacy and substitute the mix network with a Trusted Third Party Server component is considered. Due to the removal of mix network, it will optimize the data reports transmission. The addition of Trusted Third Party Server can function as a privacy-preserving agent, which can trade off the efficiency of data transmission and privacy protection. It can reduce the network hops of data reports transmission route via wireless network.

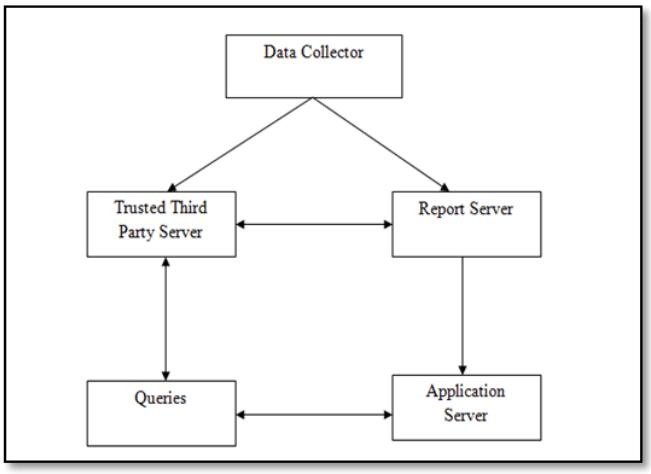

Figure 1: Proposed architecture

Context-aware data capture and carried along with each participator by data Collector. System security and participators' privacy is ensured by TTPs, stores participators' relevant information such as certificates and pseudonyms information. Report server interact with TTPs to verify the validity of the participators' identities by the certificates contained in the data reports and simplify the uploaded data reports such as data aggregation, and then send the data reports to Application Server. Application Server acts as a data Center. Queries are end users that request sensor reports in a given application, which can be personal users or community users.

5. Result/ Discussion

The expected result protects the trajectory privacy in location based services. User reveal locations to database server in a periodic or on-demand manner to obtained continuous location-based services. In snapshot spatial clocking techniques, a fully trusted party, usually termed location anonymizer is placed between both mobile user and database server. The user specified k-anonymity level or/and minimum spatial region area is satisfied.

It evaluates the privacy-preserving level of our proposal. The higher privacy level is, the stronger the trajectory privacy-preserving proposal is fig2. Consequently, the privacy leak is lower. Moreover, the privacy level, it is important to measure the privacy loss as defined. The privacy losses are the same whatever the target pseudonym the ingress pseudonym is mapping to.

References

[1] Sheng Gao, Jianfeng Ma, Weisong Shi, , Guoxing Zhan, and Cong Sun "TrPF: A Trajectory Privacy Preserving Framework for Participatory Sensing" IEEE transaction on information forensics and security, vol. 8, no. 6, June 2013.R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[2] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Commun. Mag., vol. 48, no. 9, pp. 140–150, Sep. 2010.

[3] D. Christin, A. Reinhardt, S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," J. Syst. Softw., vol. 84, no. 11, pp. 1928–1946, 2011.

[4] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Computer., vol. 2, no. 1, pp. 46–55, 2003.

[5] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location aware services," in Proc. 2nd IEEE Ann. Conf. Pervasive Computing and Communications Workshops, 2004, pp. 127–131, IEEE.

[6] C. Y. Chow and M. F. Mokbel, "Trajectory privacy in location- based services and data publication," ACM SIGKDD Exploration Newsletter, vol. 13, no. 1, pp. 19–29, 2011.

[7] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: Privacy-area aware, dummybased location privacy in mobile services," in Proc. 7th ACM Int.Workshop on Data Engineering for Wireless and Mobile Access, 2008, pp. 16–23, ACM.

[8] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Trans. Mobile Computer., vol. 7, no. 1, pp. 1–18, Jan. 2008.

[9] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. ACM 1st Int. Conf. Mobile Systems, Applications and Services, 2003, pp. 31–42.