www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10946-10948

Location Based Services: Architecture and Issues

Anshuman S. Patel[1]

[1]Information Technology Department, Government Polytechnic,
Sector-26, Gandhinagar-382026, Gujarat, India
anshu_info@yahoo.co.in

Abstract: ***Location-based services (LBS) are information and entertainment services that are accessible by mobile users through mobile networks. Examples of LBS are: Location-based traffic reports like how many cars in the free way, what is the estimated travel time to reach my destination; Location-based store finder like what are the restaurants within five miles of my location, where is my nearest fast food restaurant; Location-based advertisement like sending E-coupons to all customers within five miles of my store etc. LBS rely mainly on an implicit assumption that mobile users are willing to reveal their private locations. With untrustworthy LBS providers, the revealed private location information could be abused by adversaries. For example, an adversary may infer a user's medical record by knowing that she regularly visits a specialized clinic. Recently, there is huge interest to enable privacy-preserving LBS in which users can entertain high quality location-based services without compromising their privacy. In this paper we will discuss LBS architecture and research issues. In first section, we discuss primary concepts and different architecture of LBS. In second section we discuss research challenges and scopes.***

Keywords: Location-based services (LBS), Privacy, Security, Cryptography, Trusted third party (TTP)

1. LBS architecture and characteristics

LBS is a four layer architecture namely user interface layer, network layer, query processor layer, knowledge transfer layer. User interface layer is the physical user mobile device which consists of sensors, positioning systems which help in determining the user location by GPs. Network layer is responsible for transferring the user request to and from the service provider using the communication technology. Query processor role is performed by service provider or application provider and responsible for service request processing of the user such as nearest gas station, nearest friend etc. Knowledge base layer is responsible for maintaining the point of interest database and location information. Next, we discuss different system architectures for privacy-preserving LBS in detail.

1.1 Client-Server Architecture

This is a centralized architecture where mobile users directly communicate with the LBS provider. Existing work in this architecture can be classified into three main categories.

1.1.1 False dummies

For every location update, a user sends n different locations to the server where only one of them is true while the rest are dummies. Thus, the server cannot know which one of these reported locations is the actual one. The query processor finds an answer set that includes the answer to each location. After the user gets the answer set, she computes the exact answer.

1.1.2 False locations

The main idea is that users will send false location(s) to the server. This approach can go as simple as just sending the location of a nearby landmark or a significant object to the user location, in which the database will give the query answer with respect to the chosen landmark. A much better approach, i.e., more accurate, is Space twist. Where a user sends a nearest-neighbor query along with a false location to a database server, the database server keeps sending the nearest objects to the false location to the user. The user caches the received objects and terminates the request until the answer derived from the cached objects satisfies the user privacy and accuracy requirements.

1.1.3 Space transformation

This approach converts the original location information of data and queries into another space through a third party. The space transformation maintains the spatial relationship among the data and query, in order to provide approximate query answers or exact query answers obtained through private information retrieval.

1.2 Trusted Third Party Architecture

The main idea of this architecture is to employ a trusted third party, termed location anonymizer, to be placed between mobile users and the LBS provider. The location anonymizer is responsible for blurring user locations into cloaked areas that satisfy user's personalized privacy requirements. In this case, the user privacy requirements are mostly presented in terms of the K-anonymity model, i.e., a cloaked area A contains at least K users making each user indistinguishable among at least K users. Other location anonymization techniques employ this architecture approach for avoiding location tracking for continuous location updates or continuous queries. With the location anonymizer, the trusted third party architecture supports three new query types for privacy-preserving LBS, namely, private queries over public data (e.g., a person (private

query) asks about nearest gas station (public data)), public queries over private data (e.g., an administrator (public query) asks about the number of mobile users (private data) within a certain area), and private queries over private data (e.g., a person (private query) asks about her nearest buddy (private data)). Since the query processor embedded inside the database server does not know the actual location information of the query and/or data, it can return only an answer set that includes the exact answer to the user regardless of the actual user's location within the cloaked area. The existing privacy-aware query processing frameworks can deal with rectangular cloaked areas or circular cloaked areas as the query and/or data location information.

1.3 Distributed Architecture

In this model, mobile users communicate with each other through a fixed communication infrastructure, e.g., base stations. The basic idea of the location anonymization techniques in this architecture is that users collaborate with other peers to maintain a distributed data structure where the stored location information is used by the users to blur their location information into K-anonymous cloaked areas. Then, the query processing could be similar to the one used in the trusted third party architecture where the user sends to the server its query along with a cloaked area that includes the user location.

1.4 Mobile Peer-to-Peer Architecture

In mobile peer-to-peer networks, there is no fixed communication infrastructure or centralized/distributed servers. Instead, mobile users directly communicate with their peers through multi-hop routing to blur their locations into cloaked areas that satisfy their personalized K-anonymity and/or minimum area privacy requirements. Similar to the distributed model, the proposed peer-to-peer location anonymization technique uses the privacy-preserving query processing framework designed for the trusted third party architecture. After a user finds a cloaked area as her location, she randomly selects a peer within the cloaked area as an agent. The user sends the query along with the cloaked area to the agent, and then the agent communicates with the database server on behalf of the user. When the agent gets an answer set from the database server, the agent forwards the answer set to the user. Finally, the user computes the exact answer from the answer set.

2. Issues related to LBS

Although many research efforts have been focused on privacy-preserving LBS, there still exist many open research issues and challenges in this area that include:

2.1 Users' prospective

Existing privacy-preserving LBS frameworks are designed from the technology's prospective. There is still need to study the location privacy issue from the user's prospective. For example, how can a casual user define privacy requirements. Is it possible to define privacy levels as low, medium, and strict, and then users would choose among them. How can a user achieve a trade-off between the privacy requirements and the quality of services. How can the user evaluate the privacy risk she has from using a certain LBS.

2.2 Privacy measures and adversary attacks

There is a need to define a formal privacy measure and adversary attacks of anonymized location information in different environment settings, e.g., the Euclidean space, road network, and wireless sensor networks, and for different privacy-aware query types, e.g., static and continuous queries. Such measures and attacks can be used to evaluate the degree of privacy protection of existing and forthcoming location anonymization techniques in terms of the tradeoff between privacy and system performance.

2.3 Privacy-aware location-based query types

Existing privacy-preserving LBS frameworks support only private range and nearest-neighbor queries over public or private data. One of the future directions is to extend existing frameworks to support other kinds of location-based queries, e.g., reverse nearest-neighbor queries and aggregate nearest-neighbor queries where the query processor does not know the actual location information about the query and/or data.

2.4 Road networks environments

Existing location privacy techniques mainly consider the Euclidean space where users can move freely. In reality, most of the object movement is constrained by the underlying road network. Applying existing location privacy techniques directly to the road network environment is not practical as adversaries would have more information about the possible user locations, derived from the knowledge of the underlying road network. Thus, it is important to design new specialized location anonymization and privacy-preserving query processing techniques for road network environments.

2.5 Power consumption of the user terminal and LBS

A research area in LBS which has been explored less commonly is the power consumption for providing location related information. In a mobile environment a user should not be forced to recharge the battery of his/her mobile every now and then. The power consumptions of different location based services have been depicted. Two possible strategies recommended for reducing power consumption are: 1.decreasing the frequency of position estimations by using error models to estimate the position and 2. Use of caching to avoid frequent transmission of LBS related data.

3. Conclusion

Uses of smart applications are increasing now. With its increasing use security issues are also arising. In this paper, we discussed one of the major security issue which Location Based Services (LBS). We discussed concepts and its architecture. We also discuss different challenging issues and research scope related to LBS. LBS is one of growing research area because its architecture and privacy issues needs to be further investigated to achieve user needs.

References

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with privacygrid. In WWW, 2008.
[2] C.-Y. Chow, M. F. Mokbel, and X. Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based services. In ACM GIS, 2006.
[3] M. Duckham and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In PERVASIVE, 2005.
[4] B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. TMC, 7(1):1–18, 2008.
[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan. Private queries in location based services: Anonymizers are not necessary. In SIGMOD, 2008.
[6] G. Ghinita, P. Kalnis, and S. Skiadopoulos. Mobihide : A mobile peer-to-peer system for anonymous location-based queries. In SSTD, 2007.
[7] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In MOBISYS, 2003.
[8] M. Gruteser and X. Liu. Protecting privacy in continuous location-tracking applications. IEEE Security and Privacy, 2(2):28–34, 2004.
[9] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson. Virtual trip lines for distributed privacy-preserving traffic monitoring. In MOBISYS, 2008.
[10] J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In MOBISYS, 2004.
[11] M. F. Mokbel, C.-Y. Chow, andW. G. Aref. The new casper: A privacy-aware location-based database server (Demonstration). In ICDE, 2007.
[12] J. Voelcker. Stalked by satellite: An alarming rise in GPS-enabled harassment. IEEE Spectrum, 47(7):15–16, 2006.
[13] T. Xu and Y. Cai. Location anonymity in continuous location-based services. In ACM GIS, 2007.
[14] T. Xu and Y. Cai. Exploring historical location data for anonymity preservation in locationbased services. In INFOCOM, 2008.
[15] Kjaergaard M, “Minimizing the Power Consumption of Location-Based Services on Mobile Phones”, IEEE Pervasive Computing 8(4).
[16] Chi-Yin Chow Mohamed F. Mokbel, "Study on privacy aware location based services", Journal of scientific and Industrial research, Vol. 13, May 2013, PP. 294-299