A Survey on Anonymity in Location Based Services

Miriam Barboza-García[1], Eleazar Aguirre-Anaya[2], Gina Gallegos-García[1]

[1] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica-Culhuacan, Mexico City, Mexico
miriam.barbozag@gmail.com, ggallegosg@ipn.mx

[2] Instituto Politécnico Nacional, Centro de Investigación en Computación México City, Mexico
eaguirrea@ipn.mx

Abstract. Due to the increased use of Location Based Services (LBS), which require personal data of the user to provide the service, protecting the privacy of these data has become a challenge. An approach to provide privacy is through anonymity, by hiding the identity and location of the mobile device from the service provider or from any unauthorized party who has access at the user's request. Considering the afore mentioned, this paper gives a classification according to the architecture and approaches used in previous works, and presents a survey of solutions to provide anonymity in LBS including the open issues or possible improvements to current solutions. All of this, in order to provide guidelines for choosing the best solution approach to a specific scenery in which anonymity is required.

Keywords: Anonymity, blind signatures, cloaking areas, dummies, location based services, obfuscation, privacy.

1 Introduction

Location Based Services (LBSs) are defined as services that integrate location or position of user's mobile device with additional information so as to provide added value to a user [1]. Market trends show that LBS remain active among mobile users preferences, in this way it is important to keep looking ways for improving the privacy of these users.

The mobile device location information consists of latitude and longitude coordinates determined by a geo-location technique that can be implemented directly on the mobile device or with the active participation of the network infrastructure.

In general, a LBS architecture works as follows:

1. The user gets the mobile device position by its own means (using only the hardware on its mobile device) or with aid of some other entity (network infrastructure).
2. The user sends a request to the LBS provider (id information, location and the actual request).
3. The LBS answers the query by creating a reply message and sending it back to the mobile device.
4. The mobile user receives the reply message.

An illustration of the described architecture is shown in Figure 1.

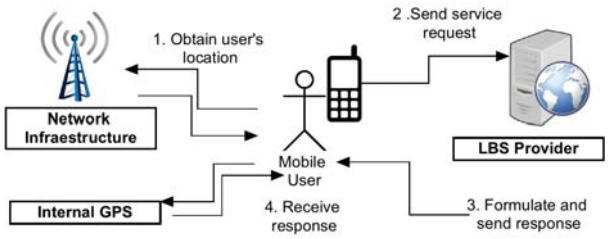

Fig. 1. Location Based Services General Architecture showing the entities that participate within the process and which actions are performed by each of them

In the described architecture, the request includes at least the user identity and the location information, assuming that this information travels in an insecure channel, it can be compromised either in its way to the service provider or when it is stored in any of the servers the LBS provider uses. Once the information is obtained, it can be used either to provide the service the user requested and/or with the intents of causing harm to the user as this information can reveal an individual's pattern of life (beliefs, preferences, activities and behavior).

The proposed solutions in the literature aim to provide the service as well as privacy to the user at the same time. These solutions can be either classified by the entities that participate in the solution or the technique they use.

The rest of the paper is organized as follows: Section 2 presents a proposed classification for the solutions that provide anonymity in LBS. Section 3 and 4 summarize some of the solutions to anonymity that have been presented in other articles, classifies the presented solutions by two approaches: cryptographic and not-cryptographic and then points out in each of them which architectural approach they implement. Section 5 gives a conclusion on the survey and possible future work.

2 Classification of Solutions

The solutions that provide anonymity can be classified either by the architecture (entities that participate to provide the solution) or by the techniques and methods they use.

2.1 Architectures to provide anonymity

The architectural solutions can be grouped into three categories [2] based on whether a third party is involved or not:

Non-cooperative or independent architecture. The mobile device by itself computes its location; it hides its identity and location using its own capability and then sends the request to the LBS provider. This is the simplest architecture but the most vulnerable to certain kinds of attacks (i.e. infecting the user´s device with a malware which alters the defined behavior to hide the data).

Centralized trust third party. It adds a trusted server that is responsible of performing the anonymizing technique, sending the request to the LBS provider and returning the result to the user. This approach is more robust in terms of privacy but the trusted server can become a potential bottleneck in the communication.

Peer to peer. This architecture consists of several mobile users trusting and cooperating with each other in order to compute their location or hiding it from untrusted entities.

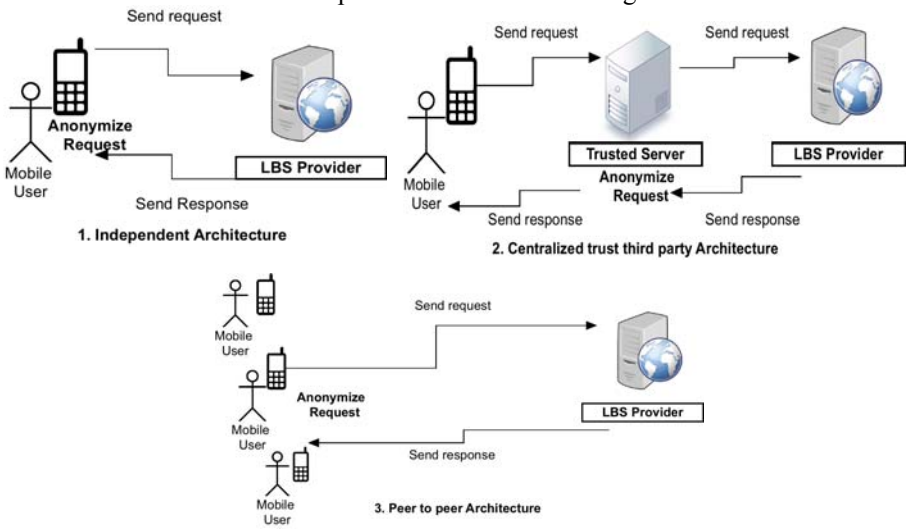

Fig. 2. Architectures to provide anonymity: Independent architecture, Centralized trust third party and Peer architecture

The Methods and Techniques to provide anonymity are described bellow:

2.2 Non-cryptographic approaches

Fake location information. Fake locations or dummies are generated and sent with the real user's location to the LBS provider; in this way the attacker cannot know for sure the true position of the user.
Cloaking techniques. A space area covering k users is formed and used to represent the user's precise location and then sent to the LBS provider.

Obfuscation Techniques. User's exact location is disguised by forwarding LBS provider less accurate location information.

2.3 Cryptographic approaches

Blind signatures. The blind signature scheme introduced by Chaum [3] is used to generate an authorized anonymous "Id" that replaces the real Id of the mobile user. This authorized anonymous id is used to make the request to the LBS.

Mix nets. Multistage system consisting of various mixes where each mix receives, decrypts and buffers messages until a number of messages have been received; once the messages are buffered the sequence of the messages is changed in a random way, encrypted and forwarded to the next mix. This procedure hides the correspondence between inputs and outputs in each mix.

Oblivious transfer. Method used in secure computing in which the sender (the LBS provider) sends some information to the receiver (the service user) but does not remember what was sent.

3 Proposed solutions using non-cryptographic approach

3.1 Fake Location Information

This set of solutions generally uses the independent architecture approach and the basic idea is to hide the user's real location among fake locations generated at the client (some dummies), before sending the request to the LBS provider. It protects user's privacy by providing k-anonymity, a metric to measure the degree of anonymity, which claims that a subject's identity is undistinguishable from at least $k - 1$ identities of other subjects.

The basic dummy technique [4] consists of a user sending its true position data with several false position data dummies to a service provider, who creates a reply message to all received position data. The user simply extracts the necessary information from the reply message. Two dummy generation algorithms are proposed.

The privacy-aware dummy-based technique (PAD) [5] seeks to improve the fact that in [4] they do not take into account the distances between dummies locations, thus they are not capable of controlling the area of the privacy region.

In [6] they deal with continuous queries (most solutions are focused on single or snap-shot queries) by injecting fake queries produced by neighbors according to user's speed and direction and with the aid of a Trusted Third Party which is responsible of finding the proper neighbors in order to achieve the k-anonymity required by the mobile user.

In MobiCache [7], mobile users form groups connected by an ad-hoc network, each time a user needs to make a query, the user first queries his group to get cached LBS related information from past queries they have made, if the cached information does not comply with the user's requirement, then the user has to make a live query to the LBS server using either the Dummy Selection Algorithm (DSA) or Enhaced DSA which guarantee that dummy locations selected have not been used before and contribute to the cache hit list in following queries.

In [8] the authors propose a Dummy-Location Selection Algorithm(DSA) which selects dummy locations using the entropy as a metric for location privacy and then spreads these dummies as far as possible so as that adversaries with side information(information about gender, social status, preferences among others) cannot figure out the real locations of the users.

The problem with these solutions is that most of the algorithms require a lot of processing power from the mobile device to produce the fake locations. If the number of dummies generated is very high, the latency in the network can increase. Other potential issue with this approach is that if the way the dummies were generated did not take into account other factors such as the environment, an attacker can end up discarding must of the dummies because it becomes too obvious that the real user was not at that place.

3.2 Spatial Cloaking

It is the most commonly used technique for protecting privacy in LBS. The basic idea is that the user's exact location can be blurred into a cloaking area that satisfies a degree of anonymity (given by a metric or specified by the user).

The solutions proposed in this area can be further classified by the architectural approach they use:

Centralized Trust Third Party Techniques

Described in [9-15], in these techniques, an anonymizer is responsible for hiding the user's exact location into the cloaked area that satisfies the privacy requirements and then sending the query to the service provider. The potential issues with these techniques are

those associated with the architecture itself, as the anonymizer can become a single point of failure and a single point of attack.

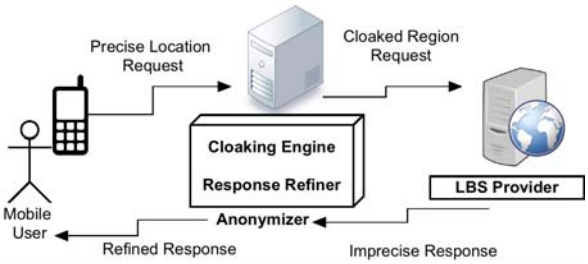

Fig. 3. Spatial Cloaking techniques with a Trusted Third Party, which computes the cloaking area and sends it to the LBS

Little variations to these techniques are presented in [16,17]: In [16] the cloaking region is generated randomly according to user's velocity and instead of sending the cloaking area, a substituted position is sent to the LBS Provider (center of the area).

In [17] the authors first use the Trusted Third Party to generate the cloaking region, once they have it they use a weighted adjacency graph (WAG) for the second phase of the method: the TTP requests the LBS Provider improved WAG information through the K-WAG Algorithm. Once the TTP has this information, it makes a selection for preferred objects and request the LBS provider for specific information about the selected objects. The LBS responds and the anonymizer can the return the response to the user.

Peer to Peer Architecture Techniques

The technique called PRIVÉ [18], a decentralized architecture for preserving the anonymity of users issuing spatial queries to LBS, provides superior k-anonymity privacy based on Hilbert space-filling which guarantees query anonymity even if the attacker knows the location of all users. They introduce a distributed protocol in which mobile entities self-organize into a faulty overlay network resembling a distributed B+ tree. The potential issue with this technique is that it may suffer from slow response time, since root-level nodes constitute potential bottlenecks.

MobiHide [19], a Peer-to-Peer (P2P) system for anonymous location-based queries in which participating mobile devices form a hierarchical distributed hash table indexing the locations of all users. The resulting system is used to construct the anonymous query belonging to K users.

Potential flaws of the solutions reviewed in [18, 19] are that they use a complex data structure that can give rise to difficulties in implementations. These issues led to the development of other solutions like the one presented in [20] where the idea is that mobile

users are able to work together to blur their locations into cloaked areas without using any fixed communication infrastructure.

In [21] authors propose a Distributed Spatial Cloaking Protocol in which users are required to build an ad-hoc network but do not need to trust each other. The initiator in the ad-hoc network chooses an agent that would be responsible of sending the query with the cloaked area to the LBS Provider.

A new approach to these techniques which also uses the spatial cloaking to achieve anonymity is the one used in [22], where the authors take advantage of Cloud Computing by replacing the Trusted Third Party by a cloud based server, in such a way that this server is in charge of computing the cloaked region but it is not trusted by the users. The communication between the users and the cloud based server is made by Orbot which is free proxy software available at Google play for android devices.

Areas of improvement in this type of techniques are that the system should remain usable even if there are less than k-users in the system and maintain the QoS even if the cloaked area becomes too large.

3.3 Obfuscation Techniques

This kind of solutions assumes the identification of users and introduces perturbations or inaccuracies into collected locations to decrease their accuracy.

In [23] the authors present three spatial obfuscation techniques to represent the user location as a circular region and using artificial perturbations of location information collected by sensing technology. The possible user locations are uniformly distributed within that region.

The algorithm Matlock presented in [24], uses matrix obfuscation, transforming the space and temporal dimensions of the location information with a small number of arithmetic operations achieving in this way low computational resources used.

In [25] path obfuscation techniques using hash chains and chains are presented. This solution is best suited for applications, which do not need to know the exact location of the user, but instead need to compute some metrics based on the information received (fitness apps, insurance apps). The user can choose to share the seed to de-obfuscate the path only to trusted users.

In [26] the authors propose using a TTP to combine ambient conditions to obfuscate the location information. The TTP uses four mechanisms to achieve this goal: First it uses r-anonymity to generate r-1 trajectories similar to the real user, then it uses the k-1 metric to produce an area containing k users, in order to avoid areas with high density, it uses the s-segment paradigm to produce a cloaked region with real world conditions and finally it uses the time obfuscation approach to confuse the LBS randomizing the query issuing time.

The possible improvements for these solutions could be: Achieving a higher degree of precision in query results, reducing the difficulty in the procedures employed, Evaluating

obfuscation techniques robustness against de-obfuscation attacks and Possibility to manage different privacy preferences expressed by users.

4 Proposed Solutions using Cryptographic Approach

4. 1 Blind Signatures

This set of solutions can be classified as using Trusted Third Party architecture, because they assume the existence of an entity besides the service provides which manages the authentication of users.

In [27] the authors present a scheme to generate an authorized anonymous ID, which replaces the real user ID. The scheme contemplates two phases: 1) Registration (generation of anonymous ID using blind signatures) and 2) Controlled Connection (Connection is provided given a valid anonymous ID is presented). An additional phase of re-confusion is introduced to replace an old anonymous ID.

In [28] the authors show a new mechanism for improving the registration and re-confusion phases in [27]. The mechanism implements blind signatures based on bilinear pairings, which seeks to delete the likability of the real ID with the authorized anonymous ID.

In [29] the authors describe a privacy protection scheme to preserve user's privacy during authentication and access control phases. It provides mutual authentication while allowing the users to anonymously interact with the desired service. They use the cryptographic primitives of blind signatures and hash chains in order to achieve these objectives through the authentication and key establishment protocols.

The solutions in [27-29] are vulnerable to a location tracking attack, where attackers analyze the moving path of a mobile user with the aid of location information, which they have collected.

In [30] an authentication protocol. It provides mutual explicit authentication between the mobile user and LBS provider and at the same time allows the user to interact anonymously. Blind signature scheme provides the generation of an authorized anonymous ID and ring signatures are used to mix the anonymous ID with a group of other authorized IDs.

The protocol claims to provide identity, location and trajectory privacy making it more robust than other solutions.

4.2 Mix Nets

Mix nets by their nature are designed to provide anonymity in communications. However most of the solutions are not applicable to the context of Location Based Services.

One exception to the afore mentioned is the proposal in [31] where the authors use a trusted proxy (anonymizer), which operates in periods of time called rounds. In each

round the requests from the users are stored. At the end of each round a series of operations are performed: generation of dummies, selection of queries based on a Binomial Distribution, cryptographic transformations and dispatching of queries to the LBS Provider.

This solution overcomes the difficulties of high latency designs and reduces imprecisions introduced by other techniques such as obfuscation or spatial cloaking. But they have to meet a minimum number of requests to be cached at the anonymizer.

4.3 Oblivious Transfer

In [32] the authors map the problem of protecting location privacy of the mobile user to an Oblivious transfer problem, where the issuer of the request receives only its corresponding reply and the service provider remains oblivious of the location of the user. Further on, they design some solutions based on different kinds of Oblivious Transfer (OT) namely Adaptive OT (implementing blind signatures), Dynamic OT and Proxy OT.

They propose the solutions but do not provide any father analysis on the correctness or feasibility of their proposals.

Based on [32], the authors in [33] propose an improved protocol by using two oblivious transfers where no third party is required to enable user's privacy.

They assume the existence of a total server, which is responsible of a group of LBS providers. The user has to perform a double OT implemented with blind signatures in order to get the key required response to the query.

This solution is thought for LBS that require payment. The computation overhead is minimum and it claims to provide higher degree of privacy compared to solutions, which use a cloaking area, or a third trusted party architecture.

5 Conclusions

It is necessary to propose new models that address new threats and attack models, which seek to break user's privacy in Location Based Services. These new models need to overcome the disadvantages of existing ones. Novel solutions approaches could combine different proposed solutions, to compensate the disadvantages of certain models with the advantages of others.

The job of updating or proposing a new survey will remain as an open task, as the development of new solutions to protect user's privacy in Location Based Services remains active; moreover it is necessary to classify the solutions by the privacy degree they offer, the attack model(s) from which they are resilient and the type of LBS to which they can be applied.

References

1. Schiller, J. Voisard, A.: Location-Based Services. Morgan Kaufmann Publishers (2004)
2. Mohaisen, A., Hong, D., Nyang, D.: Privacy in Location based services: Primitives toward the solution. NCM (2008)
3. Chaum, D.: Blind Signatures for Untraceable Payments. CRYPTO (1982) 199-203
4. Kido, H., Yanagisawa, Y., Satoh, T. An Anonymous Communication Technique using Dummies for Location-based Services. In: IEEE International Conference on Pervasive Services ICPS (2005) 88–97
5. Lu, H., Jensen, C.S., Yiu, M.L.: PAD: Privacy-Area Aware. Dummy-Based Location Privacy in Mobile Services MobiDE (2008) 16–23
6. Yao, L., et al.: Location Anonymity Based on Fake Queries in Continuous Location-Based Services. In: 7th ARES (2012) 375–382
7. Zhu, X., et al. MobiCache: When k-anonymity meets cache. In: Global Communications Conference (GLOBECOM) (2013) 9-13
8. Niu, B., Li, Q., Zhu, X., Cao, G., Li, H.: Achieving k-anonymity in privacy-aware location-based services. In: INFOCOM, 2014 Proceedings IEEE (2014) 754,762
9. Bamba, B., Liu, L., Pesti, P., Wang, T.: Supporting anonymous location queries in mobile environments with privacy grid. In: Proceedings of the International World Wide Web Conference, WWW (2008)
10. Gedik, B.,Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. In: IEEE Transactions on Mobile Computing, TMC (2008) 1–18
11. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the International Conference on Mobile Systems, Applications, and Services, MobiSys (2003)
12. Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing location-based identity inference in anonymous spatial queries. In: IEEE Transactions on Knowledge and Data Engineering (2007) 1719–1733
13. Mokbel, M.F., Chow, C.Y., Aref, W.G.: The new casper: Query processing for location services without compromising privacy. In: Proceedings of the International Conference on Very Large Data Bases, VLDB (2006)
14. Xu, T., Cai, Y.: Location anonymity in continuous location-based services. In: Proceedings of the ACM Symposium on Advances in Geographic Information Systems, GIS (2007)
15. Xu, T., Cai, Y.: Exploring historical location data for anonymity preservation in location- based services. In: Proceedings of the International Conference of the Computer and Communications Societies, INFOCOM (2008)
16. Xu, J., Yu, H., Xu C., Zheng N.: A dynamic spatial cloaking algorithm for location privacy. In: IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012) (2012) 7-9
17. Hossain, A., Hossain, A-A., Jang, S., Chang, J., Privacy-Aware Cloaking Technique in Location-Based Services. In: IEEE First International Conference on Mobile Services (MS) (2012) 24-29
18. Ghinita, G., Kalnis, P., Skiadopoulos, S.: PrivE´: Anonymous location-based queries in distributed mobile systems. In: Proceedings of the International World Wide Web Conference, WWW (2007)

19. Ghinita, G., Kalnis, P., Skiadopoulos, S.: Mobihide: A mobile peer-to-peer system for anonymous location-based queries. In: Proceedings of the International Symposium on Advances in Spatial and Temporal Databases, SSTD (2007)
20. Chow, C.Y. and Mokbel X.: Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. Geoinformatica (2011)
21. Huang Z., Xin M.: A Distributed Spatial Cloaking Protocol for Location Privacy 2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC) (2010)
22. Abbas, F., Hussain, R., Junggab S., Hasoo E., Heekuck O.: Towards Achieving Anonymity in LBS: A Cloud Based Untrusted Middleware. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom) (2013)
23. Ardagna, C. A., Cremonini, M., Damiani, E., De Capitani di Vimercati S., Samarati, P.: Location privacy protection through obfuscation based techniques. Data and Applications Security XXI, Volume 4602 (2007)
24. Wightman, P.M.; Jimeno, M.A; Jabba, D.; Labrador, M.: Matlock: A location obfuscation technique for accuracy-restricted applications. 2012 IEEE Wireless Communications and Networking Conference (WCNC) (2012)
25. Di Pietro, R., Mandati, R., Verde, N.V.: Track me if you can: Transparent obfuscation for Location based Services. 2013 IEEE 14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks (WoWMoM) (2013)
26. Hwang R., Hsueh , Y., Chung, H. A Novel Time-Obfuscated Algorithm for Trajectory Privacy Protection. IEEE Transactions on Services Computing (2014)
27. Qi, H., Wu, D., Khosla, P.: A Mechanism for Personal Control over Mobile Location Privacy. Proceedings of IEEE/ACM First International Workshop on Broadband Wireless Services and Applications, BroadWISE (2004)
28. Liao, J., Qi, Y., Huang, P., Rong, M., Li S.: Protection of mobile location privacy by using blind signature. Journal of Zhejiang University Science, vol. 7A, no. 6 (2006) 984-989
29. Ren, K., Wenjing Lou Kwangjo Kim Deng, R.: A novel privacy preserving authentication and access control scheme for pervasive computing environments. IEEE Transactions on Vehicular Technology, vol. 55, no.4 (2006) 1373-1384
30. Cao, Y., Li, Y., Li, H., Wang, X.: An Anonymous Authentication Protocol for Privacy Protection in Location Based Services. In: 4th IEEE Conference on Wireless Communications, Networking and Mobile Computing (2008) 1-5
31. Tran, M., Echizen, I., Duong, A.: Binomial-Mix-Based Location Anonymizer System with Global Dummy Generation to Preserve User Location Privacy in Location-Based Services. In: Proceedings of International Conference on Availability, Reliability and Security (2010) 580-585
32. Kohlweis, M., Gedrojc, B.: Privacy friendly location based service protocols using efficient oblivious transfer. In: Workshop uber Kryptographie (2006) 1-4
33. Kohlweiss, M., Faust, S., Fritsch, L.: Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker. In: Proceedings of 7th Workshop on Privacy Enhancing Technologies, LNCS 4776 (2007) 77-94