Privacy in Location Based Services: Protection Strategies, Attack Models and Open Challenges

Priti Jagwani[1(✉)] and Saroj Kaushik[2]

[1] School of IT, IIT Delhi, New Delhi 110016, India
jagwani.priti@gmail.com
[2] Department of Computer Science and Engineering, IIT Delhi, New Delhi 110016, India
saroj@cse.iitd.ac.in

Abstract. The increasing capabilities of position determination technologies (e.g., GPS) in mobile and hand held device facilitates the widespread use of Location Based Services (LBS). Although LBSs are providing enhanced functionalities and convenience of ubiquitous computing, they open up new vulnerabilities that can be exploited to target violation of security and privacy of users. For these applications to perform, location of the individual/user is required. Consequently they may pose a major privacy threat on its users. So for LBS applications to succeed, privacy and confidentiality are key issues. "Privacy protection" has become the buzz word now days for the users of location based services. This problem has gained a considerable attention among the researcher community also. A state-of-art survey of privacy in location based services containing details of all privacy protection schemes is presented. Further, attack models and their handling mechanism are discussed in comprehensive manner. Finally, some open challenges in the area of location privacy are also demonstrated.

Keywords: Location privacy · Attack models · Privacy protection strategies · K-anonymity

1 Introduction

Extensive usage of smart Phone and hand held devices brought the ubiquitous computing on the finger tips of users. With the tremendous growth of Internet and mobile phones the term "Location based services" has become a popular term now days. The GSM Association, simply defines Location Based services (LBSs) as services that use the location of the target for adding value to the service, where the target is the "entity" to be located (not necessarily the user of the service). Applications of widely used LBSs are enquiry and information services, traffic telematics, fleet management and logistics, location based advertising, and many more.

On one hand where life has entered in a zone of comfort and convenience because of LBS, on the other hand it has given rise to many issues like privacy, pricing, data availability, and accuracy in dealing with spatial information etc. Among all the issues addressed, privacy and security of clients using the LBS, is the most critical one. On the

K. Kim and N. Joukov (eds.), *Information Science and Applications 2017*,
Lecture Notes in Electrical Engineering 424, DOI 10.1007/978-981-10-4154-9_2

basis of the location information, user's movement, actions, priorities, ideologies and other information can be deduced. More precisely, therefore it can be said that location information jeopardizes user's identity and integrity [26].

This work presents classification of existing location privacy approaches. An overview of different types of attacks according to the knowledge applied by attacker is also presented. Previously, researchers in [2] present the privacy attacks based on categorization of anonymity and historical anonymity only and without real life examples. Authors in [17] presented the survey of various privacy preserving approaches but not of privacy attacks. Underlined work in [33] presented upright classification of attacks but failed to provide the mechanism to handle them. Therefore, the main contribution of this paper is a comprehensive presentation of attacks along with their handling mechanisms and also the open challenges lying in that particular area.

The rest of the paper is structured as follows: Sect. 2 contains details of privacy in LBS along with its need. Various privacy protection strategies are presented in Sect. 3. Section 4 consists of various attack models while Sect. 5 contains open challenges in the area of location privacy. Finally, the work is summarized in the conclusion section.

1.1 Location Privacy and Its Need

According to the Westin [34], Location privacy can be defined as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. Precisely, key factor of location privacy is control of location information. Location privacy is the ability to prevent unauthorized parties from learning one's current or past location. All the services and the location service provider (LSP) may not be trust worthy; therefore they could misuse the user data.

A complete LBS system comprises of various players such as content providers, network operators, virtual operators, service administrators, financial parties and other service providers etc. The user has to expose its location information against the services provided by the LSPs and by this at the same time user has a risk of disclosure of its personal information also. For obtaining a complete location based service, many parties are involved and thus the personal information of user is potentially known by many different services or content providers or other parties. Thus, proliferation of personal information among the different parties is difficult to control. This requires a sophisticated access control mechanism along with an appropriate authentication system.

The consequences of a location leak vary in terms of gravity. They results uncomfortable scariness of being watched or may cause unwanted revelations of a person's activities to actual physical harm. Moreover, it is actually awkward to be seen at certain places like a female clinic, crack house, AIDS clinic or a place related to a particular political ideology [20]. A user's location privacy is affected by two factors. One, what kind of location information service providers are storing about a user? and How long do they hold onto it? Well, intrusions in location privacy can uniquely identify users, more than their names or even their genetic profile and this malicious identification may lead to unsolicited situations penetrating into one's personal space.

2 Privacy Protection Strategies and Mechanisms

Several approaches have been proposed for protecting location privacy of a user. The fundamental idea behind all techniques is to prevent revelation of unnecessary information and to explicitly or implicitly control what information is given to whom and when [24, 25]. There is an inherent tradeoff between the utility and quality of LBS that users wish to receive and the location privacy they are ready to compromise. In the following sub-sections, various strategies available for privacy protection are presented.

2.1 Regulatory Strategies

All rules regarding to fair use of personal information falls under the category of regulatory approaches to privacy. In general, regulatory frameworks aim to adequately guarantee privacy protection for individuals' users. The Location Privacy Protection Act of 2011 [1] clearly states that before collecting and sharing a customer's location one needs to take his/her explicit consent.

2.2 Policy Based

Defining privacy policies and maintaining them comes under the umbrella of another class of location privacy techniques- policies based techniques. Privacy policies are trust-based mechanisms for prescribing certain uses of location information. Privacy policies define restrictions that regulate the release of the location of a user to third parties. User's needs of privacy are satisfied by restricting the ability to manage locations and disclosing information. The biggest disadvantage of policy based measures is the lack of policy enforcement specified by service provider. So despite of regulatory and policy based frameworks, adversaries are able to intrude in one's location privacy.

2.3 Location Obfuscation

Location Obfuscation is the process of degrading the quality of information about a person's location, with the aim of protecting that person's location privacy. It is the process of slightly altering, substituting or generalizing the location in order to avoid reflecting real, precise position. The most common techniques to perform obfuscation are pseudonyms, spatial cloaking, adding random noise and dummies, Redefinition of possible areas of location.

Pseudonyms, if used and implemented properly will prove to be an effective way to protect identity of users. Authors in [15] have used pseudonym for authorization and access control. It provides same level of security as that of distributed architecture and is applicable for pull based services.

In the Spatial K-anonymity paradigm [7, 25, 27], the client sends its query to middleware. It then constructs an anonymizing spatial region (ASR)/cloaking region (CR) that contains the querier's location along with other K-1 client locations. This ASR along with the query request is sent to the LBS. LBS executes the query with respect to the

ASR, and returns a superset of the results to the anonymizer, which filters out the false positives. Spatial cloaking has gained a considerable attention of privacy researchers. Rectangular cloaking regions were replaced by cloaking regions based on voronoi diagrams [18]. This provides greater flexibility, security and performance gain. Also the concept of cloaking regions containing k users as well as same cloaking region for at least k users is coined by [11]. Further k-anonymity based on fuzzy context parameters was introduced in [13]. The underline concept of k-anonymity has been extended by various approaches to increase privacy protection. The most important extensions are l-diversity, t-closeness, p-sensitivity, and historical k-anonymity.

Another approach for location privacy under the category of obfuscation is generation of dummies. To add dummy locations and noise to user's position [5, 19, 37] proposed an idea of sending additional set of dummy queries along with the actual query. The obfuscation region consists of the distinct locations included in the query set sent to the LBS.

2.4 Data Transformation

In this setting the data has been transformed using some encoding methodology like Hilbert curve etc. prior to transmitting it to the LBS. An authorized client has the secret transformation keys. This client issues an encoded query to the LBS. Both the database and the queries are unreadable by the LBS. In this way location privacy is protected.

2.5 PIR Based Location Privacy

Private Information Retrieval (PIR) protocols facilitate a client to retrieve the ith block from the server, without the server discovering which block was requested (i.e., index i). These protocols safeguard against access pattern attacks [16]. They can be grouped into: (i) information theoretic, (ii) computational [21] and (iii) secure hardware [32, 35].

There is a tradeoff between privacy and efficiency in the above mentioned techniques. While anonymity/cloaking and transformation-based approaches provide competent spatial query processing, they endure various privacy implications. On the other side of the coin there are, cryptographic and PIR-based approaches that provide significantly stronger privacy guarantees but incur more costly query processing operations.

3 Common Attacks and Challenges in Location Privacy

In order to evaluate a location privacy preserving technique/mechanism accurately, the adversary against whom the protection is required must be modeled. Hence, the adversary model is actually a very vital element of a location-privacy framework. An adversary is characterized by his knowledge and type of attack(s) he can target. An adversary model comprises of two main components: (a) the information which he/she wants to target (what he wants to infer) and, (b) the background knowledge and the inference abilities available to the adversary.

Some of the location privacy attacks along with the way to handle them and, open challenges in the respective area are given below:

Spatial Knowledge attack: Assume that a user issues a LBS request from a location p and most obviously user does not want to reveal his location. Now assume that user's location p is obfuscated by region q using some geometry-based technique. Now if adversary is aware that the user is in the obfuscated location q and q is entirely contained in the spatial extent of a particular place which is publicly known, then it can be immediately inferred that user is located in that place. However, for a professional whose work is related to that place (for him/her it's a routine), such a privacy concern would not arise because the location would be related to the user's professional activity. This privacy attack has been referred as spatial knowledge attack and has been described by Lee [22]. The spatial knowledge attack arises because real semantics of the space are ignored by geometry-based obfuscation techniques.

Handling spatial knowledge attack: These types of spatial knowledge attacks can be well handle if the privacy preservation mechanism utilizes semantics of location. These semantics may be in the form of identity of location, staying duration etc.

Location dependent attacks: Location dependent attacks may be based on continuous queries while users are moving (continous) or snapshot (one time) queries. For these queries location k-anonymity and cloaking granularity are the privacy metrics. When exact snapshot locations are unveiled, two kinds of attacks are possible: location linking attacks [11] and query sampling attacks [4]. Location linking attacks refer to the scenario where the location information included in a user query is used as a quasi-identifier to re-identify the user.

Handling location dependent attacks: The location k-anonymity model was proposed to prevent this kind of attacks by Grutser [11]. The fundamental idea is to extend an exact user location to a cloaked region that covers at least k users. Grutser used a Quad-tree based cloaking algorithm to generate cloaked regions. Ghinita [7] proposed a cloaking algorithm called hilbASR, in which Hilbert curve is used in order to approximate the spatial proximity between query requests.

Further, Cheng in [3] proposed two simple solutions, namely patching and delaying. In patching the previous cloaked area is essentially covered so that the current one is at least as large as the previous one. But obviously, drawback is increasing size of cloaking area with evolving time. The second solution, called delaying, delays the request by t time until the MBR grows large enough to fully contain the current cloaked region.

Multi query attack: As the name indicates, multi-query attack is the one where an adversary tries to identify the actual location of the query issuer with the help of a series of two or more spatial queries. All these queries involve different cloaking regions. The idea given by authors in [31] is to determine the exact location of the service requester by obtaining various cloaking regions (CR) that are shrunk or extended in succeeding queries.

Handling multi query attacks: The above mentioned problem can be addressed by ensuring reciprocity condition which ensures the users in the same anonymity set should use same CR over time. This problem can be dealt by preserving the cloaking regions for the same set of users for a specific period of time and by developing disjoint sets of users dynamically over time in order to share the common CRs.

Maximum movement boundary attack: In a maximum movement boundary attack, the adversary computes the whole area of movement of user/target, where the user could have moved between two succeeding snapshot queries or position updates. Let us assume that the initial update is sent when user was at time T1 and the other update is sent at time T2. Using this strategy the attacker can increase the precision of the update sent at T2. As only a small part of the area of T2 is reachable within the maximum movement boundary. Therefore, the remaining area of the position update can be safely excluded by the attacker.

Handling maximum movement boundary attack: Ghinita et al. [7] developed temporal and spatial transformations to sustain this type of attack. The idea of temporal transformations is to delay the requests while spatial transformations CRs are not directly generated depending on the user location, but instead are built starting from the last reported CR.

Trajectory attacks: Simply removing the identifier does not guarantee the privacy of owners while trajectory publishing. The owner might be inferred by attackers after this also. This type of attacks is called trajectory attacks [10]. The problem of trajectory anonymization is twofold. On one end the need is to preserve identity of trajectory owner and along with this the utility of published data is also to be maximized. The existing work can be classified into two categories: trajectory anonymization in free space [8, 9, 30, 35, 36] and in constrained space [9, 23]. Existing methods for location anonymization and cloaking are not applicable in this scenario.

Handling Trajectory attacks: Goal of trajectory privacy-preserving techniques is to protecting whole trajectory not to be identified by the adversary, also protecting sensitive/frequent visited locations in trajectories. This all should be done along with preserving the utility of data. However it has been shown that releasing anonymized trajectories may still have some privacy leaks. Therefore Nergiz [28] proposed a randomization based reconstruction algorithm for releasing anonymized trajectory data and also presented the adoption of this underlying techniques to other anonymity standards.

Inversion attacks: Inversion attacks are based on the situation in which a n adversary is aware of identity of k potential users of the request. Thus even after observing a specific cloaked region because of k-anonymity, adversary is not able to determine the query issuer among k users. However, if adversary knows the cloaking algorithm, he can simulate its application to the specific location of each of the candidates, and exclude any candidate for which the resulting cloaked region is different from the one in the observed request. Thus he will be able to breach the privacy of client. This type of attack

is called inversion attack. Some of the cloaking algorithms are indeed subjected to this attack.

Handling Inversion attacks: Kalnis et al. [14] show that reciprocity is the solution for this attack. Each generalization function if satisfies reciprocity will not be subjected to the inversion attack.

Query tracking attacks: In case of continuous queries, the results of query would be continuously returned for a designated time period which is called query lifetime. [4]. Query tracking attacks become possible when a user is cloaked with different users at different time instances during the query lifetime. In this way he is easily identifiable among a set of users.

Handling Query tracking attacks: Usage of memorization property is the key point to protect against query tracking attacks. According to memorization property during the whole query lifetime, the set of users being cloaked in an area should always be same [4]. Clearly, there is a line of difference between query tracking attacks and location-dependent attacks. Even if the users are prevented from query tracking attacks by applying the memorization property there is no guarantee of protection from location-dependent attacks using this.

Inference attacks: Gaining knowledge unlawfully about a subject by analyzing data is known as an "inference attack". Inference attacks on the observed queries are basically classified into two categories: tracking and identification attacks. Such attacks can lead to two types of location-privacy breaches: presence and absence disclosure. Protection strategies always aim to reduce adversary's information as little information about user locations makes it harder for the adversary to reconstruct their actual trajectories and to identify their real identities. But, unfortunately, doing so has its own cost in terms of reduced service quality for the user. Authors in [12, 20] examined location data gathered from volunteer subjects and apply four different algorithms to identify the subjects' home locations and then their identities using a freely available, programmable Web search engine.

Handling Inference attacks: Inferences attacks can be handled by different obscuration methods. Further, three different obscuration countermeasures - spatial cloaking, introducing noise, and rounding, designed to halt the privacy attacks, are applied in the above mentioned case. It has been shown in [20] that how much obscuration is necessary to maintain the privacy of all the subjects.

Other attacks: Apart from the above mentioned attacks, some other remarkable studies in the area of location privacy are: [11, 12] worked with completely anonymized GPS data. They used a standard technique from multi-target tracking. On the parallel lines the approach for anonymous indoor data is given by Williams et al. [35]. They placed simple presence sensors around a house, i.e. motion detectors, pressure mats, break beam sensors, and contact switches. These sensors helped to develop a probabilistic tracking algorithm. Using observations of sensor triggers the algorithm is detect to identify

occupant of the house around which these sensors were fixed. Duckham et al. [6] presented a model of refinement operators for working around obfuscation techniques, such as assumptions about a victim's movement constraints and goal-directed behavior.

Using the strategy of query sampling attacks an adversary may still be able to link a query to its user in case user locations are publicly known. This is possible even if locations are cloaked. This kind of attacks is called query sampling attacks [4]. Idea of k sharing regions i.e. a cloaked region should not only cover at least k users, but the region is also shared by at least k of those users is the key to protect against query sampling attacks.

4 Open Challenges and Future Research Directions

In order to solve the contradiction between location privacy protection and quality of services, researchers have already come up with a number of privacy protection methods. But there are many research issues which are still open. Following is the description of open challenges in the domain of privacy in LBS.

- **Use of semantics:** In the earlier research approaches, to attain location privacy semantics of query, data, and location itself are not considered. Very few research article paid attention to the above mentioned semantics. Research is not mature enough about the use of semantics which can bring the drastic transformation in the existing data privacy techniques.
- **Privacy-preserving Location Data Collection:** Location data generated by cell phones are collected by manufactures and published/leaked to third parties for analysis. Analysis of users' location data may cause personal privacy leakage so solutions can be research on privacy-preserving location data collection.
- **Application of PIR**: The PIR-based approaches to location privacy open pathways to a novel way of protecting user's location privacy. However, to utilize complete potential of these techniques cost of computationally intensive query processing is to be beared. Therefore, the further direction of research should be reducing the costs of PIR operations. Also "use of efficient indexing technique" for spatial queries is a future research area.
- **Formalizing of LPPM (location privacy preservation mechanism)**: All the works in the literature concentrates on solution of a particular problem of location privacy domain, e.g., protection mechanisms against a specific kind of attack, and therefore do not provide a generic framework that takes care of all location-privacy components in [29]. There exists a lack of a formal framework to quantify location privacy and to formalize attacker's model. Shokri et al. in [30] propose a framework in which they formalize various metrics and quantified location privacy. But from end user's point of view the above solution is not usable because of being cryptic so a candid formalization is still awaited.

5 Conclusion

The problem of privacy breach while using location based services has gain a considerable attention of the researchers community. This article demonstrate various achievements and research works accomplished in the area of location based privacy. However, despite of several measures to protect privacy, there are numerous attacks to intrude in location privacy and henceforth there are many open challenges still to be resolved. In this work, all such attacks and measures to prevent them have been integrated and also suggested future research directions.

References

1. The Location Privacy Protection Act of 2011 (S. 1223). https://www.franken.senate.gov/files/documents/121011_LocationPrivacyProtection.pdf
2. Bettini, C., Mascetti, S., Wang, X.S., Freni, D., Jajodia, S.: Anonymity and historical-anonymity in location-based services. In: Bettini, C., Jajodia, S., Samarati, P., Wang, X.S. (eds.) Privacy in Location-Based Applications. LNCS, vol. 5599, pp. 1–30. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03511-1_1
3. Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures. In: Proceedings of Privacy Enhancing Technology Workshop (2006)
4. Chow, C.-Y., Mokbel, M.F.: Enabling private continuous queries for revealed user locations. In: Papadias, D., Zhang, D., Kollios, G. (eds.) SSTD 2007. LNCS, vol. 4605, pp. 258–275. Springer, Heidelberg (2007). doi:10.1007/978-3-540-73540-3_15
5. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: PERVASIVE 2005 (2005)
6. Duckham, M., Kulik, L.: Simulation of obfuscation and negotiation for location privacy. In: Cohn, A.G., Mark, D.M. (eds.) COSIT 2005. LNCS, vol. 3693, pp. 31–48. Springer, Heidelberg (2005). doi:10.1007/11556114_3
7. Ghinita, G., Kalnis, P., Skiadopoulos, S.: Prive: anonymous location-based queries in distributed mobile systems. In: Proceedings of WWW 2007 (2007)
8. Gidofalvi, G., Huang, X., Pedersen, T.B.: Privacy-preserving data mining on moving objects trajectories. In: Proceedings of MDM 2007 (2007)
9. Gkoulalas-Divanis, A., Verykios, V.S.: A privacy-aware trajectory tracking query engine. SIGKDD Explor. Newsl. **10**(1), 40–49 (2008)
10. Gkoulalas-Divanis, A., Verykios, V.S., Mokbel, M.F.: Identifying unsafe routes for network-based trajectory privacy. In: Proceedings of SDM 2009 (2009)
11. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of MobiSys 03, pp. 31–42 (2003)
12. Hoh, B., et al.: Enhancing security and privacy in transaction monitoring systems. IEEE Pervasive Comput. **5**(4), 3846 (2006)
13. Jagwani, P., Kaushik, S.: Defending location privacy using zero knowledge proof concept in location based services. In: Proceedings of MDM 2012, Bangluru, India (2012)
14. Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing location-based identity inference in anonymous spatial queries. TKDE **19**(12), 1719–1733 (2007)

15. Kaushik, S., Tiwari, S., Goplani, P.: Reducing dependency on middleware for pull based active services in LBS systems. In: Sénac, P., Ott, M., Seneviratne, A. (eds.) ICWCA 2011. LNICSSITE, vol. 72, pp. 90–106. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29157-9_9
16. Khoshgozaran, A., Shahabi, C.: Private information retrieval techniques for enabling location privacy in location-based services. In: Bettini, C., Jajodia, S., Samarati, P., Wang, X.S. (eds.) Privacy in Location-Based Applications, October 2009. ISBN: 978-3-642-03510-4
17. Khoshgozaran, A., Shahabi, C.: A taxonomy of approaches to preserve location privacy in location-based services. Int. J. Comput. Sci. Eng. **5**(2), 86–96 (2010)
18. Khuong, V., Zheng, R.: Efficient algorithms for K-anonymous location privacy in participatory sensing. In: IEEE Infocom Proceedings 2012 (2012)
19. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: ICPS 2005 (2005)
20. Krumm, J.: Inference attacks on location tracks. In: LaMarca, A., Langheinrich, M., Truong, Khai, N. (eds.) Pervasive 2007. LNCS, vol. 4480, pp. 127–143. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72037-9_8
21. Kushilevitz, E., Ostrovsky, R.: Replication is not needed: single database, computationally private information retrieval. In: FOCS (1997)
22. Lee, B., Oh, J., Yu, H., Kim, J.: Protecting location privacy using location semnatics. In: KDD 2011, August 21–24, San Diego, California, USA (2011)
23. Lee, K., Lee, W.C., Leong, H.V., Zheng, B.: Navigational path privacy protection: navigational path privacy protection. In: Proceedings of CIKM 2009 (2009)
24. Liu, L.: Privacy and location anonymization in location-based services. SIGSPATIAL Spec. **1**(2), 15–22 (2009)
25. Liu, L.: From data privacy to location privacy. In: VLDB 2007, pp. 1429–1430 (2007)
26. Mokbel Mohammad, F.: Privacy-preserving location services. In: ICDM 2008 (2008)
27. Mokbel, M.F., Chow, C.Y., Aref, W.G.: The newcasper: query processing for location services without compromising privacy. In: Proceedings of VLDB 2006 (2006)
28. Nergiz, M.E., Atzori, M., Sayggn, Y., Gu, B.: Towards trajectory anonymization a generalization based approach. Trans. Data Priv. **2**(1), 47–75 (2009)
29. Shokri, R., Freudiger, J., Jadliwala, M., Hubaux, J.-P.: A distortion-based metric for location privacy. In: WPES 2009: Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, pp. 21–30, New York, NY, USA. ACM (2009)
30. Shokri, R., et al.: Quantifying location privacy. In: 2011 IEEE Symposium on Security and Privacy. IEEE (2011)
31. Talukder, N., Ahamed, S.I.: Preventing multi-query attack in location-based services. In: Proceedings of the Third ACM Conference on Wireless Network Security. ACM (2010)
32. Wang, S., Ding, X., Deng, R.H., Bao, F.: Private information retrieval using trusted hardware. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 49–64. Springer, Heidelberg (2006). doi:10.1007/11863908_4
33. Wernke, M., et al.: A classification of location privacy attacks and approaches. Pers. Ubiquit. Comput. **18**(1), 163–175 (2014)
34. Westin, A.F.: Privacy and Freedom. Atheneum, New York (1967)
35. Williams, P., Sion, R.: Usable PIR. In: NDSS (2008)
36. Xu, T., Cai, Y.: Exploring historical location data for anonymity preserving in location-based services. In: Proceedings of INFO-COM 2008 (2008)
37. You, T.H., Peng, W.-C., Lee, W.C.: Protecting moving trajectories with dummies. In: Proceedings of PALMS 2007 (2007)