글로벌경영연구
第 22 卷 2 號
2010年　8月

Security and Privacy Concerns in Location-based Services-Data Mining Perspectives

Heechang Shin[*] • June-Suh Cho[**]

Abstract

위치정보서비스는 사용자가 위치하고 있는 장소에 따라서 사용자의상황에 맞춘 서비스를 제공하여 준다. 그러나 위치정보서비스의 유용성은 인정되지만, 데이터마이닝 기법을 사용하게 되면 사용자에 대한 민감한 정보들이 누출될 가능성이 있다. 이 논문에서는 위치정보서비스를 사용하게 되면서 일어나는 이러한 위험들을 정보보안과 보호 측면에서 살펴보고, 어떠한 방법들을 통해 그러한 위험들을 방어할 수 있는지 알아보고자 한다.

Ⅰ. Introduction

Location technologies that are used by cellular phone carriers provide a good estimate of the user location, and the accuracy of location identification can be improved by using the GPS technology. Also, indoor positioning system is available based on the utilization of location sensors, wireless network, and Bluetooth. Location-based services (LBS) utilizes the location as an input to their providing services so that more personalized services can be offered based on the current user location. For example, if a user tries to find the nearest restroom in a building, the system can identify the nearest restroom from the user's current location without requiring any manual user input of location.

Recently, data mining techniques brought a lot of attention due to the rapid increase in the size of dataset. Data mining is the process of automatically searching large volumes of data for patterns using tools

[*] Graduate School of Business, Rutgers University
[**] College of Business Administration, Hankuk University of Foreign Studies

such as classification, association rule mining, clustering, etc. One popular example of data mining is that of a supermarket chain who, through analysis of transactions over a long period of time, found that beer and diapers were often bought together. However, the data mining technologies that are intended to help users may impose security and privacy threats. Data mining techniques can be applied on the location dataset to identify sensitive patterns that users would like to hide. For example, the user preference information can be found by analyzing the frequent patterns of visits to shops. If a user regularly visits a church on every Sunday morning, it can be inferred that she is a Christian. The paper surveys the security and privacy concerns of LBS, and discusses the countermeasures to such concerns.

The paper organizes as follows. Chapter 2 introduces the location based services, and chapter 3 discusses its security and privacy concerns. In chapter 4, current data mining techniques in the context of LBS are discussed, and chapter 5 briefly discusses the current security and privacy preserving techniques, and chapter 6 discusses why people share location data and implications on the LBS industry. Chapter 7 concludes the paper.

Ⅱ. Location Based Services

1. What is LBS?

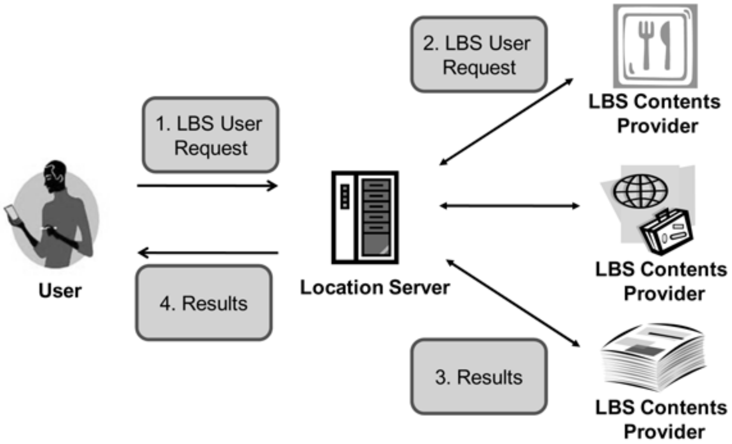
LBS refers to a service that utilizes a user’s current location to provide more customized services to users. For example, if a user visits a new place that she has never visited, the service can recommend the nearest hotel from the current location of her. Jensen et al.(2001) introduce the five main categories of applications for LBS.

1. Traffic coordination and management: Based on past and up-to-date positional data on the subscribers to a service, the service may identify traffic jams and determine the currently fastest route between two positions, it may give estimates and accurate error bounds for the total travel time, and it may suggest updated routes for the remaining travel. It also becomes possible to automatically charge fees for the use of infrastructure such as highways or bridges (termed road-pricing and metered services).

2. Location-aware advertising and general content delivery: Users may receive sales information (or other content) based on their current locations when they indicate to the service that they are in “shopping-mode.” Positional data is used together with an accumulated user profile to provide a better service, e.g., ads that are more relevant to the user.
3. Integrated tourist services: This covers the advertising of the available options for various tourist services, including all relevant information about these services and options. Services may include over-night accommodation at camp grounds, hostels, and hotels; transportation via train, bus, taxi, or ferry; cultural events, including exhibitions, concerts, etc. For example, this latter kind of service may cover opening-hour information, availability information, travel directions, directions to empty parking, and ticketing. It is also possible to give guided tours to tourists, e.g., that carry on-line “cameras.”
4. Safety-related services: It is possible to monitor tourists traveling in dangerous terrain, and then react to emergencies (e.g., skiing or sailing accidents); it is possible to offer senile senior citizens more freedom of movement; and it is possible to offer a service that takes traffic conditions into account to guide users to desired destinations along safe paths.
5. Location-based games and entertainment: One example of this is treasure hunting, where the participants compete in recovering a treasure. The treasure is virtual, but is associated with a physical location. By monitoring the positions of the participants, the system is able to determine when the treasure is found and by whom.

[Figure 1] presents the abstract view of the system architecture used in an LBS environment, and it involves the following components :

- *User* : A user brings a mobile device such as PDA or cellular phone and communicates with the contents provider via location server using wireless technologies. The location information can be acquired either by locally using GPS or from the LS, and users must communicate information about his or her location to a third party in order to receive



[Figure 1] System Architecture

useful location-based services[37].

- *Location Server* (*LS*) : LS keeps the (past as well as current) locations of users. Usually, carriers such as AT and T and Verizon assume the role of LS.
- *LBS Contents Provider* : Because the location server cannot provide all the contents for LBS such as locations of restaurants, near-by gas stations, cultural events and etc., contents providers fulfills the submitted requests, generally.

[Figure 1] illustrates the information flow between the above three components. When a user submits an LBS request to the LS (step 1), the LS forwards the request to the appropriate LBS contents provider such as location-aware advertising services or integrated tourist services (step 2). After the contents provider computes the results of the submitted request, the results are sent to the LS (step 3), which also forwards those information to the user (step 4). Although some work (i.e.(M. Duckham and L. Kulik, 2006; Ouri Wolfson, et al., 2009) considers the situation where users communicate with LBS providers directly, the three-tier architecture in [Figure 1] is general enough to model the most of scenarios that appear in this literature(M. Gruteser and D. Grunwald, 2003; B. Gedik and L. Liu, 2005; B. Gedik and L. Liu, 2008; C. Bettini, et al., 2005; C. Bettini, et al., 2007; M.F., Mokbel, et al., 2006; H. Shin, et al., 2008). As the name implies, LBS requires positioning and tracking techniques. There are a good number of ways of deciding the locations of mobile devices (i.e. GPS(C. Rizos, 2002), RF wireless LAN signals(P. Bahl and VN Padmanabhan, 2000), proximity to infrared beacons(R. Want, et al., 1992), and audio-based positioning(X. Bian, ??)). The more detailed survey of location sensing technologies can be found in(J. Hightower and G. Borriello, 2001).

Ⅲ. Security and Privacy Challenges

Location information has the potential to infer a person's personal preferences (if the location is a place where specialty products are sold or certain leisure activities can be performed), political orientation (if the location is a certain political party's office), employment status (if the location is a premise of a company), social network information (if the location is a house of one's friends), or health conditions (if the location is a specialized hospitals such as AIDS or brain cancer treatment specialization). Also, location information with corresponding time and frequencies can reveal further information about a person without any background knowledge on him/her. For example, suppose a meeting room is reserved only for faculties between 10 : 00 AM and 11 : 00 AM. If someone stays in the room over this time duration can reveal the person's profession, a professor. Also, knowing that a person visited the hospital frequently is much more meaningful than visiting the hospital only once over the last three months.

Therefore, association between location and a person can impose security and privacy threats to mobile users who subscribe to LBS. For example, there are several incidents that an adversary uses the location information to stalk a person in order to identify the personal life styles and gives a security threat to the victims by using the sensitive location information. According to(J. Voelcker, 2006), the first recorded prosecution for GPS stalking was in Boulder, Colo., in October 2000, and in 2003, another incident occurred in Kenosha, Wis. Both cases were convicted of harassment of spouse and stalking of ex-girlfriend respectively by using location-tracking devices that they hid in the victims' cars. It is expected that such threats may become more common as location sensing devices become smaller and cheaper. More worried case is that any phone can be tracked as the emergency 911 system in the U.S. requires the carriers provide GPS positioning data of its customers by tracking its customers. Although it is expected that those location information is not intentionally revealed to other third parties, there are some incidents where a person managed to obtain tracking data for an estranged spouse(J. Voelcker, 2006).

In order to breach the security and privacy of users (in other words, association between location and a person is possible), we need the following three pieces of information: i) user location dataset, ii) GIS databases, and iii) publicly available information. First, user location dataset can be available for many reasons. Location information is revealed to LBS contents providers, which is not trusted in order to enjoy the provided services from them. For example, a mobile user's request for discount information and local information require the user's current location, which is used to create such dataset. Also, the location information is being tracked and accumulated in a potentially vulnerable server. For example, traffic monitoring systems require that probe vehicles to report their current positions and other conditions about the road, which can beused to create (past as well as current) location dataset. Also, determined adversary can use localization of signals or physical observation of other users to measure the locations around the adversary. Second, there are publicly available GIS databases such as Google Maps, which provides the information about the location. For example, Google Maps provides API that displays GPS coordinates into the map and using the *what's here?* feature gives the information about that location such as address. This information can be combined with other publicly available information such as telephone directory to find about the location. For example, if the address belongs to a residence of Tom, it automatically shows that the location sample belongs to him.

One may consider that the traditional approach of pseudonymity (i.e., using a fake identity) or removing identifying information from the location dataset can guarantee the security and privacy of mobile users, but unfortunately, location itself can be used as identities of mobile users. For example, asking about the nearest restaurant to a personal house using pseudonymity can reveal the customer identity immediately by combining the location with other publicly available information such as telephone directory. In fact, data mining techniques may compromise the security and privacy although anonymous data collection is performed in the following steps :

1. Identifying the owner of location samples: There are some locations where can be used to identify an individual. For example, if a location sample belongs to a residence home, the owner can be found using the address from the telephone directory.
2. Trajectory reconstruction: Once an individual is identified, the next step is to reconstruct the trajectory of the individual from the location dataset and use them to identify sensitive places such as hospitals that can be used to reveal information about the user.

1. Identification of the owner of location samples

In order to identify a person, we need to first identifya place where there is a one-to-one mapping between the place and the person. Among the data mining techniques, clustering method is useful to identify a person from the location dataset because it can group a set of location samples that possibly belong to the same destination so that it allows automatic identification of repeatedly visited places(B. Hoh, et al., 2006). In fact, residence home satisfies such criteria. The model is presented by Baik Hoe et al.(2006), and it shows that although the identities of the locationowners are hidden, they can still be identified (even their home locations are identified). The dataset is the GPS traces from vehicles in Michigan area, and pseudo-ID is used in order to hide drivers or vehicles. The methodology to find home location can be summarized as follows :

1. Drop location samples that are too high-speed from the dataset: In residential area, a vehicle is moving very slowly, and eventually stops in front of the driver’s home location. Thus, the dataset can be filtered so that only the possible candidates for home location will be considered.
2. Apply *k*-means pair-wise clustering algorithm and store the returned cluster centroids: *k*-means pair-wise clustering algorithm is graph-based clustering algorithm, and the main advantage of the algorithm is that *k* does not need to be specified to run the algorithm. All location information is considered as initial clusters

and the algorithm keeps merging close ones into fewer clusters. The merging stops when every centroid has all its elements within a certain distance.

3. Filter the candidate home locations using the following heuristics
   - Heuristic A eliminates all centroids that don't have any evening visits (4PM-midnight): People usually go to their home in evening hours. Thus, for the purpose of finding a home location, it is useful to have a dataset with evening hours.
   - Heuristic B eliminates all centroids outside residential areas by manually inspecting satellite imagery: In order to improve the clustering result, a dataset is filtered to include only residential areas.

The result of the *k*-means pair-wise clustering algorithm correctly located about 85 percent of the homes. If a user stays in his home during the office hours, an attacker can compute the address using the GIS database and associate it with the identity of the user.

2. Trajectory Reconstruction

Once a person is identified from a location sample, trajectory from that location can be reconstructed by using target tracking algorithms(D.B., Reid, 1979; X. R., Li and V.P., Jilkov, 2001; X.R., Li and V.P., Jilkov, 2003) since location samples exhibit spatial and temporal correlation. The basic idea is that given a location sample, the next target position is decided by using the last known speed and heading information, and if there is more than one candidate, the algorithm selects the one with the highest probability of being the next sample. If the probability difference among these candidates is below the threshold, we stop the tracking. Then, the possible trajectory is reconstructed by simply linking those selected locations.

Ⅳ. Security and Privacy Threats of Data Mining Techniques

After a trajectory is reconstructed, security and privacy of users can be breached by using the data mining techniques, which can be categorized into i) user location prediction, ii) user preference classification, and iii) social network identification.

1. User Location Prediction

The Doppelganer system is developed by the MIT computer science student in order to predict where in a building a user is likely to go. In a building, location identification infrastructure is installed, and when a user with location identification device called active badge moves inside the building, the system can actually captures the current location of the user. The main application of user's future location prediction methods can be found in the cellular phone industry. A cellular phone carrier can reduce the search cost if a user's possible movement pattern can be identified because in most of cases, users will follow their historical movement patterns, and thus, in most of cases, a user's location can be found by searching only one or two regions.

When a user moves from one location to another, it is usually the same for the next time when the user begins to move from the same location, and therefore, we can predict a user's next location based on her current as well as previously visited locations(Website, 2008). User movement can be modeled as a Markov stationary process of order *r*, which assumes that the location can be predicted from the sequence of *r* most recently visited locations. The Markov model is useful for describing user mobility because it allows for reasonably accurate predictions with relatively small memory requirement. Song et al.(2006) found that low-order Markov models performed as well or better than the more complex and more space-consuming compression-based models.

Although the prediction model is useful to a user because when a user reaches a location, the system can provide to-do list that is applicable to future locations of the user trips, it may cerate security and privacy concerns among the users since attacks can be performed on predicted future locations as well as the past and current locations.

2. User Preference Classification

User preference can be classified by analyzing the spatio-temporal location information along with context information. Sparacino presented an interesting system in the context of museum(F. Sparacino, 2002). Visitors of a museum are equipped with a small device that stores the voice records of different versions of descriptions for exhibits in the museum. When a user moves along, and stops in front of an exhibit in the museum, the system recognizes the current location of the user, and the description of the exhibit is played. The system classifies the user as greedy, selective, or busy based on the pattern of time that she spends viewing the exhibit. If the user is classified as greedy, the longest version of description is played, and the playing time of description is getting shorter if the classification is selective or busy, respectively. Bayesian network is used for the classification method.

GPS signal's accuracy is lower in the urban area because a building blocks the signal. By using this heuristic, Ashbrook and Starner cluster places where the GPS signal was lost, which can be potentially significant locations to the users(D. Ashbrook and T. Starner., 2003), and Marmasse considers additional input such as dwell time, breaks in time or distance, and periods of low GPS accuracy to identify such locations(N. Marmasse, 2004). More recent approaches(J.H., Kang, 2005; E. Kaasinen, 2003) use clustering techniques with extra consideration on time and location to finds such information and shows better results. User preference classification can reveal of a person's preferences and personal life styles, which incurs security and privacy threats as we described in the previous section.

3. Social Network Identification

Social network can be identified if a group of people's spatio-temporal location history is available using spatiotemporal co-occurrence pattern mining techniques(M. Celik, et al., 2008; H.W., Lauw, et al., 2005; F. Qian, 2009; Z. Zhang and W. Wu, 2008). For example, Lauw et al. (H.W., Lauw, et al., 2005) identify the social network by using spatio-temporal co-occurrence association. The basic idea of the algorithm is based on the assumption that if the number of occurrences of two people ismore than the random number of occurrences, they would have social relationships. The support measure of a social relationship between two users is the number of all the events that two users are at the same place and spend more than the predefined time. If this counted support measure is more than the threshold, it is considered that two users have a relationship. The security and privacy issues of forming a social network are obvious. For example, if the social network information of a company is revealed to a competitor, new product development information may be revealed if the network includes a renowned researcher whose research area is not directly related to the current product line of the company. Also, if the social network information of a company is revealed to a competitor, new product development information may berevealed if the network includes a renowned researcher whose research area is not directly related to the current product line of the company. Also, consider the study of Klovdahl et al.(AS Klovdahl, et al., 1994) which analyzed the social network structure of “a population of prostitutes, injecting drug users (IDU) and their personal associates in a moderate-sized city.” In this example, the relationship between two individuals represents a sexual interaction or the use of a shared needle, which clearly breaches the privacy of users included in the network.

V. Security and Privacy Preserving Techniques

In this section, we briefly present the different techniques that have been proposed to address the security and privacy issues.

- Access control: Advanced access control models can be used in the context of LBS to enforce security and privacy rules. The privacy policies for the use of the location data defined by users are enforced by the location services. Youssef et al.(M. Youssef, et al., 2005) introduced the access control model that users define authorizations which service providers can provide access location and profile of users based on the time and space that the user is located.
- Temporal and spatial generalization (anonymization): The de-identification of data or the separation of identifying values from sensitive data can be used to defense the attacks. Gruteser and Grunwald(2003) first defined location k-anonymity as the state in which location information of a mobile user is indistinguishable from the location information of at least k-1 other mobile users. his is a direct application of k-anonymity (P. Samarati and L. Sweeney, 1998) to the LBS environment and can be achieved by using a trusted third party (such as the location server) to generalize the location to a spatio-temporal region that includes at least k mobile users. Gedik and Liu(2008) extend this work toprovide personalized location k-anonymity, allowing each user to specify their own

k. Mokbel et al.(2006) utilize a similar model but propose a different implementation based on a multi-level grid-based index structure to allow more efficient anonymization and nearest neighbor queries. Recently, Shin et al.(2008) proposed a profile anonymization model that ensures privacy while delivering personalized location based services that are based on user profiles.

Recently, the concept of location *k*-anonymity has been extended to trajectory data, called trajectory *k*-anonymity models (O. Abul, et al., 2008; Mehmet Nergiz, 2008). Essentially, trajectory *k*-anonymity is ensured if there exist at least *k* trajectories (or subset of trajectories) within the anonymized region similar to location *k*-anonymity. Abul et al.(2008) utilize uncertainty of GPS measures to ensure *k*-anonymity for trajectory data by moving some trajectory points from the original location to another location. However, in continuous LBS environment, the answer generated by the LBS provider cannot guarantee the correctness of the answer to the users by using this method. The trajectory *k*-anonymity in(Mehmet Nergiz, 2008) is achieved by generalizing each location point of *k* trajectories, resulting in a set of GRs. However, these approaches are not suitable for continuous LBS environment since their methods only apply to historical trajectory data by considering trajectory data publication case.

- Prevention of Critical Location Traces: Privacy risk increases as the time duration of tracking increases: in fact, Hoh et al.(2007) evaluate the degree of privacy risk based on how long an adversary can follow an object in a data set and use suppression methods to ensure the privacy of users. Bresford et al.(2005) presented a privacy preserving technique, mix zone. The main idea of mix zone is that whenever a user enters in a mix zone, their identity is changed so that an attacker cannot match the identities of users with the previous location history after they visited a mix zone. Bettini et al.(2005) extend location *k*-anonymity to include historical traces of location information of mobile users. Xu and Cai(2007) propose two anonymization techniques, plain and advanced, to guarantee the anonymity of users in continuous LBS environment. Essentially, the plain approach ensures that every GR contains the same users that were being included within the initial GR when the first request has been made. However, this is impractical in reality because the movement pattern of users would be different as time elapses, thus generating GR too large in the later requests. The advanced approach relaxes this constraint and may contain other users, which are not included in the initial GR. Chow and Mokbel (2007) propose a generalization technique, called dynamic group, such that the GR for each mobile user in a group is the spatial region that includes all users in the group. In general, a user is not allowed to issue a query unless the user belongs to a certain group. Users may be added to or removed from some groups. However, all existing work assumes that answers to the requests are repeatedly evaluated until the service expires.

Ⅵ. Discussion

1. Sharing of Location Information

One potential solution for security and privacy is to perform all processing of location information locally on the mobile device, and do not share location information with other entities. However, this approach is not suitable because of the following limitations(M. Duckham and L. Kulik, 2006).

- Limited Computational Power: The processing power of hand-held devices is usually not efficient enough to perform complex spatiotemporal queries locally.
- Limited Infrastructure Capabilities: The spatial data sets tend to be large, and the wireless network bandwidth may not enough to communicate spatial data between the server and the mobile devices in a real-time manner.
- Characteristics of Spatial Data: Spatial data sets are still expensive to collect and collate, and thus, the data would not be revealed to the public unless it is really required.

- Data Integrity and Concurrency Problems: These issues are inevitably associated with maintaining copies of the same data sets across multiple mobile devices.

Therefore, information needs to be shared with other parties in LBS environments.

2. Implications on LBS Industry

In order to use an LBS, a user trades their services with sensitive location information. This trade-off can be extreme. For example, a user does not provide his location data to any entity and therefore, he does not enjoy any service benefits (0% service). Another extreme is that a user always provides his exact location to other entities, which gives him 100% of service. In general, a user wants to enjoy the benefits from the LBS while certain level of privacy and security is guaranteed. For example, a user who is willing to provide his location data without identifying information is allowed to enjoy additional discount. This finding actually calls for research into users' perceived usefulness in exchange for giving up their location information.

A social study(S. Consolvo, et al., 2005) shows that participants rejected 23% of the 3,798 requests for their location information. The main reason of rejection is that those users perceive the possible privacy breach due to the provided location information. For example, employees are disturbed by the request from their managers during non-work hours. Also, many participants do not want to disclose location information when they are running errands or doing something that they are not supposed to do. This study shows that there are two different types of users with respect to the location information: i) security and privacy insensitive and ii) security and privacy sensitive users. For example, there are employees who do not provide their location information even during the work hours while some workers choose to disclose the location information to their boss on Saturday.

LBS industry has an implicit assumption that users agree on revealing their private user locations. However, studies show those users' concerns about privacy and security is the main reason to prohibit enjoying such services. Therefore, LBS industry may lose their business opportunities to those who are sensitive to the security and privacy issues. Also, even the second group may not care about the privacy and security issues because they are insensitive to the negative consequences of a location leak(J. Krumm, 2009). However, if there are more public attention to the incidents of LBS usage such as stalking(J. Voelcker, 2006; Website, 2009; Website, 2005; Website, 2004), it is possible for them to perceive the privacy and security implications of providing location information, and therefore not to subscribe LBS any further.

Ⅶ. Conclusion

Location based services (LBS) require a user's current location and its location traces to provide the service. While LBS may be helpful to the user, data mining techniques can identify sensitive patterns so that they can represent security and privacy threats. In this paper, the threats from LBS are identified, and general prevention techniques are introduced.

We can address security issues by enforcing access control policies in order to prevent unauthorized access to important resources, but enforcing security does not automatically guarantee the privacy issues because the second use of the revealed location to the authorized users are not enforced. Thus, it calls for integrating privacy and security of a mobile user within a common framework. Access control mechanism and anonymization improve on the results in terms of security and privacy issues separately, it is still unclear that pursuing individual solutions for each topic can ensure privacy and security at the same time. More specifically, it calls for development of a metric that can measure the trade-offs between privacy and security enforcement. In other words, the release of the information according to the security enforcement can result in the privacy breach of the users because location information is considered as sensitive, and therefore, should consider the amount of privacy leakage. This is not easy to solve because the background knowledge of attackers are not known when access control decisions are made. Existing work addresses this issue by management of secondary use of released data, but it is still unclear that the enforcement strictly follows the data handling policies after the access has been granted. Also, existing privacy-defense mechanisms use oversimplifying assumptions about the attacker, and background knowledge such as movement direction, profiles, and future trajectory is ignored during processing anonymization. Therefore, existing work cannot ensure complete privacy for users, and it is required to develop a comprehensive family of anonymity modelsthat incorporate mobile users' location, direction, profile, and future trajectory information. In addition, while protecting location privacy, the quality of service (QoS) of LBS plays an important role and should be preserved. Formal analysis and experimental results is required to demonstrate that the proposed anonymization techniques in fact guarantee privacy and service quality with nominal computational cost.

References

[1] Man accused of stalking ex-girlfriend with gps. Website, 2004. http://www.foxnews. com/story/0,2933,131487,00.html.

[2] Man arrested for stalking wife with gps. Website, 2005. http://crime.about.com/b/2005/02/14/man-arrested-for-stalking-wife-with-gps.htm.

[3] Predict user mobility in enterprise networks. Website, 2008. Predict user mobility in enterprise networks.

[4] Onalaska man accused of using gps for stalking. Website, 2009. http://archives.chicagotribune.com/2009/may/19/news/chi-ap-wi-gpsstalking.

[5] O. Abul, F. Bonchi, and M. Nanni, "Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases," In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, (2008), pp.376-385.

[6] D. Ashbrook and T. Starner., "Using GPS to learn significant locations and predict movement across multiple users," *Personal and Ubiquitous Computing*, Vol.7. No.5(2003), pp.275-286.

[7] P. Bahl and VN Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings, IEEE,* Vol.2. 2000.

[8] A.R., Beresford, Location privacy in ubiquitous computing, *IEEE Pervasive Computing*, 2005.

[9] C. Bettini, S. Mascetti, and X.S., Wang, "Privacy Issues in Location-based Services," 2007.

[10] C. Bettini, X.S., Wang, and S. Jajodia, "Protecting privacy against location based personal identification," In *Proceedings of the 2nd VLDB Workshop on Secure Data Management*, (2005), pp.185-199.

[11] X. Bian, G.D., Abowd, and J.M., Rehg, "Using sound source localization in a home environment," *3rd International Conference on Pervasive Computing (Pervasive),* pp.19-36.

[12] M. Celik, S. Shekhar, J.P. Rogers, and J.A. Shine, "Mixed-Drove Spa-

tiotemporal Co-Occurrence Pattern Mining," *IEEE Transactions on Knowledge and Data Engineering*, (2008), pp.1322-1335.

[13] C.Y., Chow and M.F., Mokbel, "Enabling private continuous queries for revealed user locations," *Lecture Notes in Computer Science*, 4605:258, 2007.

[14] S. Consolvo, I.E., Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations: why, when, and what people want to share," In *Proceedings of the SIGCHI conference on Human factors in computing systems*, (2005), pp.81-90. ACM New York, NY, USA.

[15] M. Duckham and L. Kulik, "Location privacy and location-aware computing," *Book chapter in Dynamic and Mobile GIS : Investigating Change in Space and Time*, (2006), pp. 35-51.

[16] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," *Distributed Computing Systems, 2005. ICSCS 2005 Proceedings. 25th IEEE International Conference on*, (2005), pp.620-629.

[17] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, (2008), pp. 1-18.

[18] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," In *Proceedings of the 1st international conference on Mobile systems, applications and services*, (2003), pp.31-42. ACM Press New York, NY, USA.

[19] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *Computer*, Vol.34. No.8(2001), pp.57-66.

[20] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," *IEEE Pervasive Computing*, Vol. 5. No.4(2006), p.46.

[21] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving Privacy in GPS Traces via Uncertainty-Aware Path Cloaking," *14th ACM Conference on Computer and Communications Security*, 2007.

[22] C.S., Jensen, A. Friis-Christensen, T.B., Pedersen, D. Pfoser, S. Saltenis, and

N. Tryfona, "Location-based services-a database perspective," *Proceedings of Scandinavian GIS*, Vol.30. 2001.

[23] E. Kaasinen, "User needs for location-aware mobile services," *Personal and Ubiquitous Computing*, Vol. 7. No.1(2003), pp.70-79.

[24] J.H., Kang, W. Welbourne, B. Stewart, and G. Borriello, "Extracting places from traces of locations," *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol.9. No.3(2005), p.68.

[25] AS Klovdahl, JJ Potterat, DEWoodhouse, JB Muth, SQ Muth, and WWDarrow, "Social networks and infectious disease: The Colorado Springs study," *Social Science and Medicine*, Vol.38. No.1(1994), pp.79-88.

[26] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, Vol.13. No. 6(2009), pp.391-399.

[27] H.W., Lauw, E.P., Lim, H. Pang, and T.T., Tan, "Social network discovery by mining spatio-temporal events," *Computational and Mathematical Organization Theory*, Vol. 11. No.2(2005), pp.97-118.

[28] X.R., Li and V.P., Jilkov, "A Survey of Maneuvering Target Tracking? Part III: Measurement Models£," In *Proceedings of SPIE*, Vol. 4473(2001), p.424.

[29] X.R., Li and V.P., Jilkov, "Survey of maneuvering target tracking," Part I: Dynamic models. *IEEE Transactions on Aerospace and Electronic Systems*, Vol.39. No.4(2003), pp.1333-1364.

[30] N. Marmasse, "*Providing Lightweight Telepresence in Mobile Communication to Enhance Collaborative Living*," PhD thesis, Massachusetts Institute of Technology, 2004.

[31] M.F., Mokbel, C.Y., Chow, and W. G., Aref, "The new Casper: query processing for location services without compromising privacy," In *Proceedings of the 32nd international conference on Very large data bases*, VLDB Endowment, (2006), pp. 763-774.

[32] Mehmet Nergiz, Maurizio Atzori, and Yucel Saygin, "Towards Trajectory Anonymization: a Generalization-Based Approach," In *Proceedings of First ACM GIS Workshop on Security and Privacy in GIS and LBS*, 2008.

[33] F. Qian, Q. He, and J. He, "Mining

Spread Patterns of Spatio-temporal Cooccurrences over Zones," In *Proceedings of the International Conference on Computational Science and Its Applications*: *Part II*, (2009), p.692.

[34] D.B., Reid, "An algorithm for tracking multiple targets," *IEEE Transactions on Automatic Control*, Vol. 24. No.6(1979), pp.843-854.

[35] C. Rizos, "Introducing the global positioning system," *Manual of geospatial science and technology*, (2002), pp.77-94.

[36] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," *Proceedings of the IEEE Symposium on Research in Security and Privacy*, 1998.

[37] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," *Computer*, Vol.36. No.12 (2003), pp.135-137.

[38] H. Shin, V. Atluri, and J. Vaidya, "A profile anonymization model for privacy in a personalized location based service environment," In *Proceedings of the 9th International Conference on Mobile Data Management* (*MDM08*), (2008), pp.73-80.

[39] H. Shin, V. Atluri, and J. Vaidya, "A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment," *The 9th International Conference on Mobile Data Management* (*MDM*), 2008.

[40] L. Song, D. Kotz, R. Jain, and X. He, "Evaluating next-cell predictors with extensive Wi-Fi mobility data," *IEEE Transactions on Mobile Computing*, Vol.5. No.12(2006), pp.1633-1649.

[41] F. Sparacino, "The Museum Wearable: real-time sensor-driven understanding of visitors' interests for personalized visually-augmented museum experiences," In *Proceedings of Museums and the Web* (*MW2002*), *April*, Citeseer, (2002), pp.17-20.

[42] J. Voelcker, "Stalked by satellite-an alarming rise in gps-enabled harassment," *Spectrum, IEEE*, Vol.43. No. 7(2006), pp.15-16.

[43] R. Want, A. Hopper, V. Falc∼ao, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems* (*TOIS*), Vol. 10. No.1(1992), pp.91-102.

[44] Ouri Wolfson, Divyakant Agrawal, and Chang-Tien Lu, editors, *17th ACM*

SIGSPATIAL International Symposium on Advances in Geographic Information Systems, ACM-GIS 2009, November 4-6, 2009, Seattle, Washington, USA, Proceedings. ACM, 2009.

[45] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," In *Proceedings of the 15th annual ACM international symposium on Advances in geographic information systems*. ACM New York, NY, USA, 2007.

[46] M. Youssef, V. Atluri, and N.R., Adam, "Preserving mobile customer privacy: an access control system for moving objects and customer profiles," ACM Press New York, NY, USA, (2005), pp.67-76.

[47] Z. Zhang and W. Wu, "Composite Spatio-Temporal Co-occurrence Pattern Mining," In *Proceedings of the Third International Conference on Wireless Algorithms, Systems, and Applications*, (2008), p.465.