ISSN 23499842(Online), Volume 1, Special Issue 1(NCFCSIT 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

PRESERVING LOCATION TRANSFORMATION BASED GEO-SOCIAL APPLICATION

MS.ANUJA MARY JOSE[1], MS.D.RAJAKUMARI[2],M.Sc.
[1]Assistant professor, [2]PG Scholar(M.E),
[1,2]CSE Department, Aksheyaa College of Engineering, (Anna University), kanchipuram, Tamil Nadu, India
[1]anuja.amj@gmail.com, [2]raja19.kumari@gmail.com

Abstract—**Using geo social applications, such as Four Square, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce Technique, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that Technique provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.**

Index Terms—**Mobile Computing, Privacy Protection, Smart Phone, Location Privacy, Location Transformation, Privacy mechanism**

I. INTRODUCTION

With billions in downloads and annual revenue, Smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. Within these markets, a new wave of geo social applications is fully exploiting GPS location services to provide a "social" interface to the physical world. Examples of popular social applications include social rendezvous, local friend recommendations for dining and shopping, as well as collaborative network services and games. The explosive popularity of mobile social networks such as SCVNGR and Four Square (3 million new users in 1 year) likely indicate that in the future, social recommendations will be our primary source of information about our surroundings. Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geo social applications operate on fine-grain, time-stamped location information. For current services with minimal privacy mechanisms, these data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real-world examples where the unauthorized use of location information has been misused for economic gain, physical stalking, and to gather legal evidence. Even more disturbing, it seems that less than a week after Face book turned on their popular "Places" feature for tracking users' locations, such location data were already used by thieves to plan home invasions. Clearly, mobile social networks of tomorrow require stronger privacy properties than the open-to-all policies available today. Existing systems have mainly taken three approaches to improving user privacy in geo social systems: 1) introducing uncertainty or error into location data, 2) relying on trusted servers or intermediaries to apply anonymization to user identities and private data, and 3) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user.

In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive

to deploy on mobile devices, and even on the servers in answering queries such as nearest neighbor and range queries.

The challenge, then, is to design mechanisms that efficiently protect user privacy without sacrificing the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers. More specifically, we target geo social applications, and assume that servers (and any intermediaries) can be compromised and, therefore, are untrusted. To limit misuse, our goal is to limit accessibility of location information from global visibility to a user's social circle. We identify two main types of queries necessary to support the functionality of these geo social applications: point queries and nearest neighbor queries.

Points queries query for location data at a particular point, whereas queries query for nearest data around a given location coordinate (or up to a certain radius). Our goal is to support both query types in an efficient fashion, suitable for today's mobile devices. To address this challenge, in this paper, we propose LocX (short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here onward). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data. Thus, we can partition location data based on users' social groups, and then perform transformations on the location coordinates before storing them on un trusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is only available to the members of the social group.

To address this challenge, in this paper, we propose LocX (short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here on- ward). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data. Thus, we can partition location data based on users' social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, al- lowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on LocX lightweight and suitable for running on today's mobile devices.

The rest of the paper is organized as follows. Section II describes about the scenarios and requirements and section III shows related work. Section IV shows the system design. Section V shows the details of Implementation and section VI describes about the conclusion of this paper.

II SCENARIOS AND REQUIREMENTS

Here we describe several scenarios we target in the context of emerging geosocial applications that involve heavy interaction of users with their friends. We use these scenarios to identify the key requirements of a geo-social location privacy preserving system.

2.1 Geo-social Application Scenarios

Scenario 1. Alice and her friends are excited about exploring new activities in their city and leveraging the "friend referral" programs offered by many local businesses to obtain discounts. Alice is currently in downtown and is looking to try a new activity in her vicinity. But she also wants to try an activity that gives her the most discount. The discounts are higher for a user that refers more friends or gets referred by a friend with high referral count. As a result Alice is interested in finding out the businesses recommended by her friends and the discounts obtained through them, within her vicinity. In addition, she is also interested in checking if there are discounts available for her favorite restaurant at a given location. Scenario 2. Alice and her friends are also interested in playing location-based games and having fun by exploring the city further. So they setup various tasks for friends to perform, such as running a few miles at the Gym, swimming certain laps, taking pictures at a place, or dining at a restaurant. They setup various points for each task, and give away prizes for the friends with most points. For Alice to learn about the tasks available near her, she needs to query an application to find out all tasks from friends near her and the points associated with them. The

scenarios above, while fictitious, are not far from reality. Groupon and LivingSocial are some example companies that are leading the thriving business of local activities. SCVNGR [6] offers similar services as location- based games. But none of these services provide any location privacy to users: all the locations visited by the users are known to these services and to its administrators. Our goal is to build a system that caters to these scenarios and enables users to query for friends' data based on locations, while preserving their location privacy. We want to support: 1) point query to query for data associated with a particular location, 2) circular range query to query for data associated with all locations in a certain range (around the user), and 3) nearest-neighbor query to query for data associated with locations nearest to a given location. Finally, while it is also useful to query for data that belongs to nonfriends in certain scenarios, we leave such extensions for future.

2.2 System Requirements

The target scenarios above bring out the following key requirements from an ideal location-privacy service: Strong location privacy. The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited. . Location and user unlinkability. The servers hosting the services should not be able to link if two records belong to the same user, or if a given record belongs to a given user, or if a given record corresponds to a certain real-world location. . Location data privacy. The servers should not be able to view the content of data stored at a location. . Flexibility to support point, circular range, and nearest-neighbor queries on location data. . Efficiency in terms of computation, bandwidth, and latency, to operate on mobile devices. The need for each of these requirements becomes more clear when we describe the related work and their limita- tions in more detail in the next section. In our proposed system, LocX, we aim to achieve all these requirements.

III RELATED WORK

3.1 Prior Work on Privacy in General Location-Based Services (LBS)

There are mainly three categories of proposals on providing location privacy in general LBSs that do not specifically target social applications. First is spatial and temporal cloaking [11], [12], [13], [22], [15], wherein approximate location and time is sent to the server instead of the exact values. The intuition here is that this prevents accurate identification of the locations of the users, or hides the user among k other users (called k-anonymity [12], [13], [22]), and thus improves privacy. This approach, however, hurts the accuracy and timeliness of the responses from the server, and most importantly, there are several simple attacks on these mechanisms [23], [24], [25], [26] that can still break user privacy. Pseudonyms and silent times [27], [14] are other mechanisms to achieve cloaking, where in device identifiers are changed frequently, and data are not transmitted for long periods at regular intervals. This, however, severely hurts functionality and disconnects users. The key difference between these approaches and our work is that they rely on trusted intermediaries, or trusted servers, and reveal approximate real-world location to the servers in plain text. In LocX, we do not trust any intermediaries or servers. On the positive side, these approaches are more general and, hence, can apply to many location-based services, while LocX focuses mainly on the emerging geosocial applications. The second category is location transformation, which uses transformed location coordinates to preserve user location privacy. One subtle issue in processing nearest- neighbor queries with this approach is to accurately find all the real neighbors. Blind evaluation using Hilbert Curves [21], unfortunately, can only find approximate neighbors. To find real neighbors, previous work either keeps the proximity of transformed locations to actual locations and incrementally processes nearest-neighbor queries [28], or requires trusted third parties to perform location transfor- mation between clients and LBSA servers [29]. In contrast, LocX does not trust any third party and the transformed locations are not related to actual locations. However, our system is still able to determine the actual neighbors, and is resistant against attacks based on monitoring continuous queries [30], [31]. The third category of work relies on PIR [16] to provide strong location privacy. Its performance, although im- proved by using special hardwares [17], is still much worse than all the other approaches, thus it is unclear at present if this approach can be applied in real LBSs.

3.2 Prior Work on Privacy in Geo-social Services

For certain types of geo-social services, such as buddy tracking services to test if a friend is nearby, some recent proposals achieve provable location privacy [18], [19] using expensive cryptographic techniques such as secure two party computation. In contrast, LocX only uses inexpensive symmetric encryption and pseudorandom number generators. The closest work to LocX is Longitude [32], [33], which also transforms locations coordinates to prevent disclosure to the servers. However, in longitude, the secrets for transformation are maintained between every pair of friends to allow users to selectively disclose locations to friends. As in, longitude can let a user reveal her location to only a subset of her friends. In contrast, LocX has a simpler threat model where all

friends can access a user's informa- tion and hence the number of secrets that users have to maintain is only one per user. LocX can still achieve location and user unlinkability. In addition, LocX can provide more versatile geosocial services, such as location-based social recommendations, reminders, and others, than just buddy tracking as in the above prior work.

3.3 Anonymous Communication Systems

These systems, including Tor [34], provide anonymity to users during network activity. One might ask, then, why using Tor to anonymously route data to LBSA servers is not sufficient? This approach seems to provide privacy as the server only sees location data but not the identity of the user behind that data. However, recent research has revealed that hiding the identity of the users alone is not sufficient to protect location privacy. Even if Tor is used, it is possible for an attacker with access to the location data to violate our privacy and unlink ability requirements. For example, using anonym zed GPS traces collected by the servers, it has been shown that users' home and office locations, and even user identity can be derived [23], [24], [25], [26]. LocX defends against such attacks and meets all our requirements.

3.4 Systems on Untrusted Servers

In the context of databases, recent systems proposed running database queries on encrypted data (stored on untrusted servers), using heavy-weight homomorphic [35] or asymmetric encryption [36] schemes. These approaches are suitable for spatial data outsourcing or data mining scenarios where the data are static and are owned by limited number of users. But they are less suitable for LBSAs, where the data are dynamic and personal, and thus cannot be encrypted under a single secret key. In the context of location and social applications, Persona [37] and Adeona [38] also relied on encrypting all data stored on untrusted servers to protect user privacy. Persona focused on privacy in online social networks, and Adeona focused on privacy in device tracking systems where there is no data sharing among users. Applying Persona's mechanisms to LBSAs directly would encrypt all location coordinates, making LBSAs unable to process nearest-neighbor queries. But if location is not encrypted, attacks using anonymized GPS traces, mentioned above, can succeed, making Persona insufficient to protect location privacy. Similarly, Adeona is useful for a user to retrieve her own data, but not the data from her friends. Our contributions complement these systems. Some techniques in these papers can help LocX as well, for example, Persona's approach to partition data shared with friends into fine-grained groups, and Adeona's hardware-assisted approaches to speed up crypto processing.

IV SYSTEM DESIGN

In this section, we describe the design of LocX in detail. Location coordinates refer to the longitude, latitude pairs associated with real-world locations. A pair of coordinates is returned from a GPS, and is used to associate data with a location. Location data or location information refers to such data associated with a location. For example, when reviews (and referral point details) are written for a given restaurant, the reviews are the location data associated with the restaurant's location coordinates.

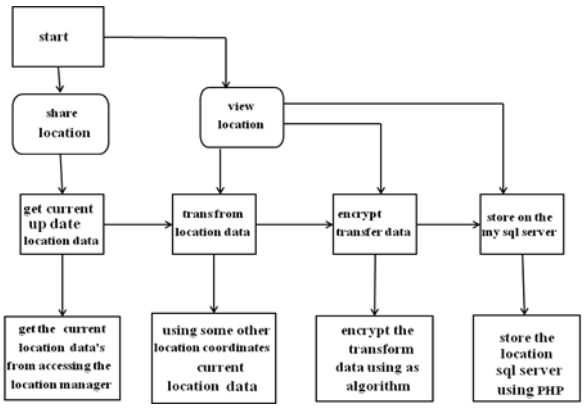

Fig. 1 System architecture

System and attacker model. In this paper, we assume that the companies that provide LBSA services manage the servers. Users store their data on the servers to obtain the service. The companies are responsible for reliably storing this data, and providing access to all the data a user should have access to displaying ads, or charging users some usage fees. In our attacker model, we assume that the attacker has access to the LBSA servers. This attacker could be an employee of the company running the service or an outsider that compromises the servers. The attacker might even be an oppressive regime or a government that obtains data from the providers via subpoenas. As a result, in our model, the attacker can access all the data stored on the servers, and can also monitor which user device is accessing which pieces of information on the servers. Our goal is to design a system that preserves the location privacy of users in this setting. We assume that the attacker does not perform any attacks on the consistency or integrity of data on the servers, but aims only to learn users' location information. Finally, like all prior social systems [39], [40], [41], [37], we assume that the friends of a user are trusted and do not collude with the servers in breaking the user's privacy.

V IMPLEMENTATION

We are using an AES encryption technique to encrypt the transforms location data's. We are using a some key to encrypt the location transformed data as. He crypto extension uses as to secure offline data storage by encrypting the backing MySQL database data's. Using the encrypted data store is very similar to the default implementation explained in the Caching and Offline guide, although there are two additional classes provided to replace existing functionality. When defining your Offline Policy and Offline Store, use the Secure Offline Store class which will encrypt all data before it is written to the database: If your app does navigation or tracking, you probably want to get the user's location at regular intervals. While you can do this with Location Client. Get Last Location (), a more direct approach is to request periodic updates from Location Services. In response, Location Services automatically updates your app with the best available location, based on the currently-available location providers such as WiFi and GPS. To get periodic location updates from Location Services, you send a request using a location client. Depending on the form of the request, Location Services either invokes a callback method and passes in a Location object, or issues an Intent that contains the location in its extended data. The accuracy and frequency of the updates are affected by the location permissions you've requested and the parameters you pass to Location Services with the request.

A. LOCATION UPDATER

If your app does navigation or tracking, you probably want to get the user's location at regular intervals. In response, Location Services automatically updates your app with the best available location, based on the currently-available location providers such as Wi-Fi and GPS. To get periodic location updates from Location Services, you send a request using a location client. Depending on the form of the request, Location Services either invokes a callback method and passes in a Location object, or issues an Intent that contains the location in its extended data. The accuracy and frequency of the updates are affected by the location permissions you've requested and the parameters you pass to Location Services with the request.

Fig. 2 shows that main menu view for the application in the mobile. Preserving location Privacy is the application name and through which it activates.

Fig. 2. View Application

B. ENCRYPT

We are using a AES encryption technique to encrypt the transforms location data's. we are using a some key to encrypt the location transformed data's. He crypto extension uses AES to secure offline data storage by encrypting the backing MySQL database data's. Using the encrypted data store is very similar to the default implementation explained in the Caching and Offline guide, although there are two additional classes provided to replace existing functionality.

Fig. 3 Encryption

C. LOCATION TRANSFORM

After getting the location updater data's the location transform function is occurred. The location

transform mean we change the current location data using some other degree values. so using these values the original location data was changed to another faked location data's. In response, Location Services automatically updates your app with the best available location, based on the currently-available location providers such as WiFi and GPS. To get periodic location updates from Location Services, you send a request using a location client.

Fig. 4 Enter Secret key to store Location Data

Depending on the form of the request, Location Services either invokes a callback method and passes in a Location object, or issues an Intent that contains the location in its extended data. The accuracy and frequency of the updates are affected by the location permissions you've requested and the parameters you pass to Location Services with the request. Fig. 4 shows the encryption and secret key to store location data.

D. SECRETS KEY

Each user they want to share their location they muster enter their name and the corresponding secret key for that user name. After entering the secret key and the name the users location data was stored on the our server, if any one they want to access other locations data's they must enter their name and their corresponding secret key for accessing their location data's otherwise the user cannot view the other users locations data.

A fundamental activity in land surveying is the integration of multiple sets of geodetic data, gathered in various ways, into a single consistent data set, that is into a common geodetic reference frame. In the past it was sufficient, but in some cases also unavoidable, to combine all such data using a locally, mostly arbitrarily, defined geodetic datum. In recent years, a growing trend toward the use of satellite positioning and global mapping satellite systems has been developed providing position – based products in a world reference frame.

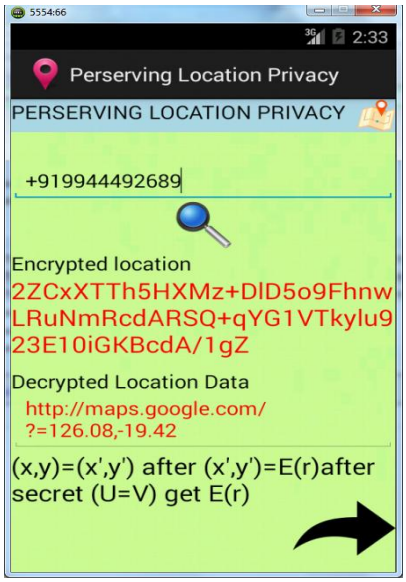

Fig. 5 View Location Page

One of the principal purposes of such a world frame is to eliminate the use of multiple geodetic dataum. But, until such a world geodetic reference frame is accepted, used and implemented worldwide, the satellite data may lead to several practical difficulties when the results need, also, to be related to a geodetic datum, as is often the case. Such problems arise in several instances, such as navigation, revision of older maps, cadastral surveying, industrial surveying, deformation studies, geo-exploration etc. In general, the necessity of transforming data from one reference frame to another is solved by applying a coordinate transformation. Although coordinate transformations. Are straightforward mathematically, they may cause several problems when applied, for various reasons, such as poor knowledge of the distortions and inconsistencies of the local datum, or even lack of sufficient knowledge of geodesy of people who use such transformations.

To properly understand coordinate transformations in geodesy, it is essential to understand the relationship between a geodetic reference system, which is mathematically established, and its realization, via geodetic observations, the GRF (Geodetic Reference Frame).

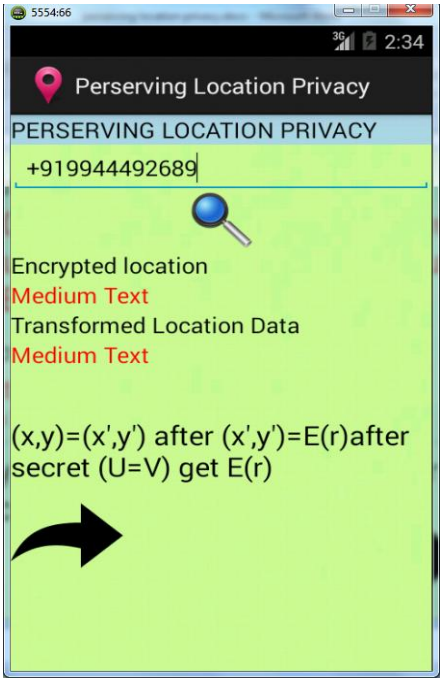

Fig. 6 Decryption of Location Data

Naturally, the GRF has some degree of uncertainty, due to observational errors in the determination of the coordinates of the ground points.

Fig. 7 View Location Map

The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access.

VI CONCLUSION

Users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user's data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties. We have presented Zero square, a location for building geo-social applications that is designed with privacy as the primary feature. Secondary goals include being able to support various application use cases and not requiring unreasonable amounts of computation from a mobile device. We have discussed the API of the entities in our system and shown how applications can be built using these functions. We have also provided a working implementation of Zero square and proof of-concept applications. Our experimental results demonstrate real-world practicality of Zero square. Future work includes weakening the assumptions made in our threat model (e.g., defending against actively malicious U, L, or C) and enabling users to continuously check in with L without them becoming identifiable or tractable. Furthermore, In location privacy the location privacy was protected from the servers and other hackers. But sometimes we need to send our location and other details to the particular members to emergency situation. so we develop a module that is used to capture the picture with our camera the after that the picture should convert a geo tagged picture with a particular message. That picture will send automatically to the police office department servers. We use a complexity algorithm for to secure the users locations data and the users personals information's that is related to the geo information that personal information will automatically encrypt before send to another person.

REFERENCES

[1] M. Motani, V. Srinivasan, and P.S. Nuggehalli, "*PeopleNet: Engineering a Wireless Virtual Social Network*," Proc. ACM Mobi Com, 2005.

[2] M. Hendrickson, "*The State of Location-Based Social Networking on the iPhone*," based-social-networking-on-the-iPhone, 2008.

[3] P. Mohan, V.N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones," Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008.

[4] G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath,

"Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.

[5] M. Siegler, "Foodspotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/ food spotting, 2013.

[6] "SCVNGR," http://www.scvngr.com, 2013.

[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.

[8] F. Grace, "Stalker Victims Should Check for GPS," http:// www.cbsnews. Com, Feb. 2003.

[9] A. Gendar and A. Lisberg, "How Cell Phone Helped Cops Nail Key Murder Suspect. Secret 'Pings' that Gave Bouncer Away," New York Daily News, Mar. 2006.

[10] "Police: Thieves Robbed Homes Based on Facebook, Social Media Sites," WMUR News, http://www.wmur.com/r/24943582/ detail.html, Sept. 2010.

[11] M. Gruteser and D. Grunewald, "Anonymous Usage of LocationBased Services through Spatial and Temporal Cloaking," Proc. First Int'l Conf. Mobile Systems, Applications Services, 2003.

[12] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007.

[13] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems, 2005.

[14] T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy in Wireless Lans," Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.

[15] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[16] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizes Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data, 2008.

[17] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.

[18] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011.

[19] G. Zhong, I. Goldberg, and U. Hengartner, "Louis Lester and Pierre: Three Protocols for Location Privacy," Proc. Seventh Int'lConf. Privacy Enhancing Technologies, 2007.

[20] N. Daswani and D. Boneh, "Experimenting with Electronic Commerce on the Palmpilot," Proc. Third Int'l Conf. Financial Cryptography, 1999.

[21] A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy," Proc. 10th Int'l Conf. Advances Spatial Temporal Databases, 2007.

[22] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. 16th Int'l Conf. World Wide Web, 2007.

[23] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Pervasive Computing, 2009.

[24] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing Magazine, vol. 5, no. 4, pp. 38-46, Oct. 2006.

[25] B. Hoh et al., "Preserving Privacy in GPS Traces via Uncertainty Aware Path Cloaking," Proc. 14th ACM Conf. Computer Comm. Security, 2007.

[26] J. Krumm, "Inference Attacks on Location Tracks," Proc. Fifth Int'l Conf. Pervasive Computing, 2007.

[27] A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004.

[28] M.L. Yiu, C.S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the Trade Offs among Location Privacy Query Performance and Query Accuracy in Mobile Services," Proc. IEEE 24th Int'l Conf. Data Eng., 2008.