Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.38 – 44

A SURVEY ON PRESERVING LOCATION PRIVACY

Nishant B.Chobitkar
Research Scholar, IT Department
SCOE, Vadgaon (BK)
Pune, Maharashtra, India
Nishant.chobitkar@gmail.com

Abstract- Location is well blended with man. His positions are always accompanied by where he has been. In the eruption of the social applications of the current era, man cannot avoid sharing his location information. On the other hand, even when he prefers to go social, man is worried about preserving his privacy. For many privacy reasons, men prefer to keep his location uniqueness safe and secure. Security breaches in geo-social applications may lead to user tracking, home invasions etc. Research activities and studies have contributed their share to the area of security. This is a survey on the work done in association with privacy conservation in location based services.

Keywords: Location discovery, Privacy in location based services.

I. INTRODUCTION

We survive in a planet in which closeness is formed practically by the present technology. Man is frequently engaged in this irresistible number of online activities that have manage to make a social-world around us. While still debating on the boons and banes of these applications, it is a stand-alone fact that these are prone to security breaches. Hustle- especially related to location privacy is in a high due to the interest generated by many new geo-social applications. We are drawn to them due to their fun-with-facts approach. Since smart phones have managed to reach the pockets of laymen, location-based services are of more demand. Location detection devices like GPS enable the users to send the co-ordinate information to a location based data-server. The location details can be provided by the service providers even though it might lack pin-pointed accuracy. Users check-in from their locations to avail the location based services. Friend finders, location-based games, place-reviews etc. result in the exchange of huge amount of location data. If this information is misused, it can lead to tracking of users and unauthorized access to their privacy. With its help, detailed activities of the users can be inferred or their daily movements can be predicted. The most concerning drawback of today's geo-social applications is the privacy problem presented by the frequent use of localization features on smartphones. A user must provide her location to an application provider in order to request information from an application or use its features. An application provider can build up large amounts of location data along with timestamps indicating when the user made a request. This data allows the provider to localize users (know their location at a particular point in time), build up traces of users' movement, and even track users. The provider may also have identifying information and attributes (such as interests) that users have provided during registration or are part of their profiles in a social application. This data can be stored over a long time period and aggregated or statistically analyzed. Knowledge of a user's location at particular times, especially when combined with other information about the user, can be used by the provider to learn more about the user than she may have intended

when signing up. An alarming amount of information, such as a user's home and work locations, activities, and relationships can be inferred from data that a provider has. 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 Facebook turned on their popular "Places" feature for tracking users' locations, such location data was 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. The security of location information is thus a matter of concern. Many studies over the last years have contributed fruitful shares to thwart this problem. They have suggested methods with varying perspectives to achieve the unanimous goal of privacy. This literature survey focuses on the work done in connection with privacy in location based services.

II. LITERATURE SURVEY

Gruteser et al. uses spatial and temporal cloaking [1] wherein estimated location and time is send to the server instead of the correct values.

Methodology:

A system model and a quadtree-based algorithm were introduced to guarantee k-anonymous position information during reductions in location declaration. In the system model, the mobile nodes converse with outer services through a middle anonymity server that is element of the trusted computing base. In an initialization phase, the nodes will set up an authenticated and encrypted connection with the anonymity server. When a mobile node sends position and time information to an external service, the anonymity server decrypts the message, removes any identifiers such as network addresses, and perturbs the position data according to the cloaking algorithms to reduce the reidentification risk. Moreover, the anonymity server acts as a mixrouter , which randomly reorders messages from several mobile nodes, to prevent an adversary from linking ingoing and outgoing messages at the anonymity server. Finally, the anonymity server forwards the message to the external service.

Algorithm: (Adaptive-Interval Cloaking Algorithm)

The key idea underlying this algorithm is that a given degree of anonymity can be maintained in any location—regardless of population density—by decreasing the accuracy of the revealed spatial data. The algorithm is inspired by quadtree algorithms. It subdivides the area around the subject's position until the number of subjects in the area falls below the constraint k_{min}. The previous quadrant, which still meets the constraint, is then returned.

Issues:

Hurts the accuracy and correctness of the responses from the server, and most importantly, there are several simple attacks on these mechanisms that can still break user privacy.

K.Srinivasan,C.Chandrasekar[2]employs pseudonyms and silent times to achieve cloaking, where in device identifiers are changed frequently, and data is not transmitted for long periods at regular intervals.

Methodology:

This approach obfuscates three sources of location privacy leakage: sender identity, time of transmission and signal strength. To prevent an attacker from using user identity for tracking, users must use frequently changing pseudonyms for communications. During a silent period, a user does not send any wireless transmissions. In an opportunistic silent period, the user's machine detects that it has not transmitted for a period in excess of the silent period, and uses that time to change pseudonyms. Uses transmit power control to minimize the number of APs in range while ensuring at least one AP for connectivity. Allows each user to configure her privacy requirements as policies and to have user-friendly operations that result in minimal disruption while satisfying the users' privacy policy. The system implements the opportunistic silent period and keeps track of the time period between communication sessions. When that period exceeds the silent period, a new MAC address is requested from the AP using a transmit power decodable only by the serving AP.

Issues:

Severely hurts functionality and disconnects users.

In [3] the proposed system, Relies on trusted servers or intermediaries to protect user privacy.

Methodology:
Casper consists of two components, namely, the location anonymizer and the privacy-aware query processor. The location anonymizer is a trusted third party that receives continuous location updates from users, blurs the location updates to cloaked spatial areas, and sends the cloaked areas to the location based database server. While cloaking the location information, the location anonymizer also removes any user identity to ensure the pseudonymity of the location information. The privacy-aware query processor is embedded inside the location-based database server to tune its functionality to deal with anonymous queries and cloaked spatial areas rather than the exact location information. Based on the stored data, three novel query types are supported in Casper through its privacy aware query processor:
a. Private queries over public data where the query issuer location is private while the data objects are public,
b. Public queries over private data where the query issuer location is public while the data objects are private, and
c. Private queries over private data where both the query and data object locations are private.
Issues:
A risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators.

In [4], Papadopoulos et al. makes use of Private Information Retrieval (PIR) to provide strong location privacy.
Methodology:
Focuses on k nearest neighbor (kNN) queries and define the notion of strong location privacy, which renders a query indistinguishable from any location in the data space. There are two main components in the scheme: (i) the PIR functionality, and (ii) the query plan. The former ensures that the LBS is oblivious of each block retrieved by the algorithms. The query plan ensures that every query retrieves the same number of blocks during its execution. Suppose that a server maintains a database consisting of N sequential blocks. PIR protocols enable a client to retrieve the ith block from the server, without the server discovering which block was requested (i.e., index i). Constructed benchmark method, called BNC and AHG by optimizing and generating a query plan in order to enforce strong location privacy.
Issues:
Its performance is much worse than all the other approaches.

S. Mascetti, C. Bettini, and D. Freniet al.[5] Transforms location coordinates to prevent disclosure to the servers.
Methodology:
Longitude is a privacy-aware centralized solution based on a three-party secure computation involving only communication between each buddy and the server. Each time a user location is sent to the Service Provider (SP), it is first generalized to a two-dimensional area A whose dimension depends on the user privacy requirement with respect to buddies. The solution considers a mapping from the two-dimensional space in which users move into a toroidal space. A solid transformation is applied to the projection of A in the toroidal space and the result is then sent to the SP. Each user shares a (possibly different) secret with each of her buddies that determines the solid transformation. The SP computes proximity in the toroidal space and communicates the result to the participating buddies, which can then compute the proximity in the two-dimensional space.
Issues:
In Longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends. Longitude can let a user reveal her location to only a subset of her friends.

Motani et al. depicts a wireless virtual social network [6] which mimics the way people seek information via social networking.
Methodology:
PeopleNet is a simple, scalable and low-cost architecture for efficient information search in a distributed manner. It uses the infrastructure to propagate queries of a given type to users in specific geographic locations, called bazaars. Within each bazaar, the query is further propagated between neighboring nodes via peer-to-peer connectivity until it finds a matching query. The PeopleNet architecture can overlay easily on existing cellular infrastructure and entails minimal software installation. Three metrics were identified for system performance:
a. probability of a match,
b. time to find a match

c. number of matches found by a query.
Two simple models, called the swap and spread models, were described for query propagation within a bazaar. The architecture could be easily integrated into the existing cellular infrastructure. Exploits the natural mobility of people and their interactions with other people to pair up matching queries.

Issues:

The security aspects of such a network were not thoroughly studied.

B. Gedik and L. Liu [7] presents a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing.

Methodology:

Provided a unified privacy personalization framework to support location k-anonymity for a wide range of users with context-sensitive personalized privacy requirements. This framework enables each mobile node to specify the minimum level of anonymity it desires as well as the maximum temporal and spatial resolutions it is willing to tolerate when requesting for k-anonymity preserving location-based services (LBSs). An efficient message perturbation engine was devised which runs by the location protection broker on a trusted server and performs location anonymization on mobile users' LBS request messages, such as identity removal and spatial-temporal cloaking of location information. A suite of scalable and yet efficient spatio-temporal cloaking algorithms, called CliqueCloak algorithms, were developed to provide high quality personalized location k-anonymity, aiming at avoiding or reducing known location privacy threats before forwarding requests to LBS provider(s).

Issues:

Introduction of uncertainty into location data thereby degrading the results returned.

Narayanan et al. describes privacy-preserving tests for proximity [8].

Methodology:

Introduction of a set of desiderata for privacy-preserving proximity testing. Reduction of private proximity testing to the underlying cryptographic problem of private equality testing (PET). Use of location tags to enhance the security of private proximity testing. A location tag is an ephemeral, unpredictable nonce associated with a location and can be derived from various electromagnetic signals available in the environment, such as Wi-Fi and Bluetooth. It can be thought of as a shared pool of entropy between all users at a given location at a given time. Designed and implemented a key agreement system using a social network as a key-distribution mechanism, instead of traditional PKI. The system binds the user's public key to the user's social network account.

Issues:

Deployment of cryptographic techniques by the location based services. The scalability while applying to geo-social applications.

PRIV´E [9] is a decentralized architecture for preserving the anonymity of users issuing spatial queries to LBSs.

Methodology:

Mobile users self-organize into an overlay network with good fault tolerance and load balancing properties. PRIV´E avoids the bottleneck caused by centralized techniques both in terms of anonymization and location updates. The state is distributed in numerous users, rendering the system resilient to attacks. We assume a large number of users who carry mobile devices (e.g., mobile phones, PDAs) with embedded positioning capabilities (e.g., GPS). The devices have processing power and access the network through a wireless protocol such as WiFi, GPRS or 3G. Moreover, each device has a unique network identity (e.g., IP address) and can establish point-to-point communication (e.g., TCP/IP sockets) with any other device in the system through a base station (i.e., the two devices do not need to be within the range of each other). For security reasons, all communication links are encrypted. In addition, we assume the existence of a trusted central Certification Server (CS), where users are registered. Prior to entering the system, a user u must authenticate against the CS and obtain a certificate. Users having a certificate are trusted by all other users. Typically, a certificate is valid for several hours; it can be renewed by recontacting the CS. Apart from the certificate, the CS returns to u the IP addresses of some users who are currently in the system. u employs this list to identify an entry point to the distributed network. The CS does not know the locations of the users and does not participate in the anonymization process. Each user corresponds to a peer and peers are grouped into clusters, based on their location. Within each cluster, peers elect a cluster head, and the set of heads is grouped recursively to form a tree. For load balancing, the cluster heads change periodically in a round-robin manner. Typically users ask Range or Nearest-Neighbor (NN) queries with respect to their position (e.g., "find the nearest hospital"). Based on individual criteria, users select the required degree of anonymity K. K may vary among consecutive queries. Users collaborate to achieve

spatial cloaking and construct the K-ASR in a distributed manner. Then, a random user u0 is selected to send the anonymized query to LBS, filter the result set and forward the actual answer to the query initiator. The result set from the LBS is a superset of the actual answer and its cardinality depends on the size of the K-ASR.

Issues:

PRIV´E uses hierarchical clustering of mobile users, but the requirements of total ordering and annotation impose particular challenges that have not been addressed.

According to B. Hoh et al. anonymous position information [10] can be made available at the traffic-monitoring service.

Methodology:

Addresses privacy by separating the communication and authentication tasks (which rely on pseudonyms or identities) from data analysis and sanitization (which require access to detailed position information). To resolve the tension between data integrity and privacy, the architecture assigns the authentication and filtering functions and the actual data analysis to separate entities. One entity knows the vehicle's identity but can't access precise position and speed information; the other entity knows position and speed but not identity. The architecture relies on encryption to prevent eavesdropping, tamper-proof hardware to reduce the risk of node compromise and spyware installation, and data sanitization to further strengthen data integrity. The Communication Server maintains network connections and authenticates users but doesn't access location and speed data. The Traffic Server receives anonymous data from the Communication Server, decrypts and sanitizes it, and computes the real-time congestion maps.

Issues:

This technique cannot be applied directly to geo-social applications. Several simple attacks on the server can break user privacy.

A. Beresford and F. Stajano[11] enhances user privacy in location-based services by preventing the tracking of long-term user movements.

Methodology:

The model assumes the existence of a trusted middleware system, positioned between the underlying location system(s) and untrusted third-party applications. Applications register interest in a geographic space with the middleware known as the application zone. Users register interest in a particular set of location-aware applications and the middleware limits the location information received by applications to location sightings of registered users located inside the application zone. Each user has one or more unregistered geographical regions where no application can trace user movements; such areas are called mix zones, because once a user enters such a zone, user identity is mixed with all other users in the mix zone. A boundary line is defined as the border between a mix zone and an application zone.

Applications do not receive a traceable user identity associated with a location sighting, but instead receive a pseudonym. The pseudonym allows communication between user and application; such communication must pass through a trusted intermediary to prevent trivial linking of a pseudonym with an underlying user identity. The pseudonym of any given user changes whenever the user enters a mix zone.

Issues:

Reveals approximate real world location to the servers in plain-text.

Persona [12] is an Online Social Network where users dictate who may access their information.

Methodology:

Persona hides user data with attribute-based encryption (ABE), allowing users to apply fine-grained policies over who may view their data. Provides an effective means of creating applications in which users, not the OSN, define policy over access to private data. Each Persona user generates an asymmetric key-pair and distributes the public key out-of-band to other users with whom they want to share data. These other users are referred as friends, though the nature of each relationship is defined by the user. Persona allows users to create groups and choose which users are parts of a given group. Users control access to personal data by encrypting to groups. Restricting data to specific groups allows users to have fine-grained control over access policy, which permits exchanging data with more restrictions. Cryptographic primitives in Persona allow users to flexibly specify and encrypt to groups. Users may specify groups using arbitrary criteria, but we expect users to choose groups based on transparent relationships such as neighbor or co-worker. Groups created by one user do not affect the groups that can be created by another. However, to support OSN communication patterns, the groups created by one user should be available for use, not just for decryption, but also for encryption, by friends.

Issues:

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, and making Persona insufficient to protect location privacy.

Sr No.	Authors Name	Methods	Drawback
1	M.Gruteser and D. Grunwald(2003)	spatial and temporal cloaking	Less accuracy and correctness
2	K.Srinivasan, C.Chandrasekar(2012)	high boost filter and Gaussian filter	Harmed performance and disconnect user
3	M. F. Mokbel, C.-Y. Chow, and W. G. Aref(2007)	Casper:location anonymizer and the privacy-aware query processor	Private data can be exposed
4	S. Papadopoulos, S. Bakiras, and D. Papadias(2010)	Private Information Retrieval	Degrade perfomance
5	S. Mascetti, C. Bettini, and D. Freni(2009)	Longitude protocol	Not appropriate for range queries over moving objects
6	M. Motani, V. Srinivasan, and P. S. Nuggehalli(2005)	Swap and spread models, were described for query propagation	Security aspect of a network were not in detail studied
7	B. Gedik and L. Liu(2007)	k-anonymity model for protecting location privacy	Degrading results
8	A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh(2011)	cryptographic protocols	Problem while applying to geo-social applications.
9	G. Ghinita, P. Kalnis, and S. Skiadopoulos(2007)	decentralized architecture for preserving the anonymity of users	ordering and annotation impose particular challenges not addressed
10	B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady(2006)	Data suppression techniques	Several simple attacks on the server can break user privacy
11	A. Beresford and F. Stajano(2004)	Mix zones- using an anonymity service that delays and reorders messages from subscribers within pre-defined zones	Reveals approximate real world location to the servers in plain-text
12	R. Baden, A. Bender, N. Spring, B. Bhattacharjee(2009)	Encryption of data on servers	Insufficient to protect location privacy
13	T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno(2008)	provides strong guarantees of location privacy while preserving the ability to track missing devices	useful for a user to retrieve her own data, but not the data from her friends

Table no.1: Survey on preserving location privacy

T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno system [13] deals with private methods to assist in the recovery of lost or stolen Internet-connected mobile devices. Adeona provides strong guarantees of location privacy while preserving the ability to efficiently track missing devices.

Methodology:

The client consists of two modules: a location-finding module and a cryptographic core. With a small amount of state, the core utilizes a forward-secure pseudorandom generator (FSPRG) to efficiently and deterministically encapsulate updates, rendering them anonymous and unlikable, while also scheduling them to be sent to the remote storage at pseudo randomly determined times (to help mitigate timing attacks). The core ensures forward-privacy: a thief, after determining all of the internal state of the client and even with access to all data on the remote storage, cannot use Adeona to reveal past locations of the device. The owner, with a copy of the initial state of the client, can efficiently search the remote storage for the updates. The cryptographic core uses

only a sparing number of calls to AES per update. Provides a device tracking system not tied to a particular service provider. Adeona employs OpenDHT as the third party service, resulting in an immediately deployable system that does not rely on any single trusted third party.

Issues:

Adeona is useful for a user to recover her own information, but not the information from her associates.

III. CONCLUSION

Privacy in location based services is a major issue that draws apprehension. As location sensitive devices pass through, it become significant to assess privacy threats and countermeasures in connection with location data. This data can be used to harm a person economically, invite unwanted advertisements, enable stalking or physical attacks, or infer embarrassing proclivities. The data and location details of the user thus need to be protected from unauthorized access and misuse. This literature survey was done on the papers that deal with privacy preservation in location based services. Introducing noise into the location data, relying on trusted parties, using cryptographic techniques etc. are the major solutions offered to tackle the problem of location privacy. Active researches are going on in this field to augment the scope and extend of privacy achieved. Let us be hopeful that these studies would cover the way for more protected geo-social application.

REFERENCES

[1]. M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. of Mobisys, 2003.

[2]. K. Srinivasan, C. Chandrasekar,An Efficient Fuzzy Based Filtering Technique for Finger- print Image Enhancement, AJSR,ISSN 1450- 223X,no.43, pp. 125-140, 2012.

[3]. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: A privacy aware location-based database server," in ICDE, 2007.

[4]. S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest neighbor search with strong location privacy," PVLDB, 2010..

[5]. S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized privacy preserving computation of users' proximity," in Proc. of SDM, 2009.

[6]. M. Motani, V. Srinivasan, and P. S. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in Proc. of MobiCom, 2005.

[7]. B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. of ICDCS, 2005.

[8]. A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, Location privacy via private proximity testing," in Proc. of NDSS, 2011.

[9]. G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location based queries in distributed mobile systems," in Proc. of WWW, 2007.

[10]. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," in IEEE Pervasive Computing Magazine, 2006.

[11] A. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in Proc. of Pervasive Computing, 2004.

[12]. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin,"Persona: An online social network with user defined privacy," in Proc.of SIGCOMM, 2009.

[13]. T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno, "Privacy preserving location tracking of lost or stolen devices: Cryptographic techniques and replacing trusted third parties with DHTs," in Proc. Of USENIX Security Symposium, 2008

