Study on Privacy Aware Location based Service

K.B. Priya Iyer\textsuperscript{1} and V. Shanthi\textsuperscript{2}

\textsuperscript{1}MOP Vaishnav College for women (Autonomous), Chennai
\textsuperscript{2}Dept of M.C.A, St. Joseph College of Engineering, Chennai, India

Received 28 July 2012; revised 15 December 2012; accepted 04 March 2013

The recent technology drive in communications, positioning and geographical systems opens novel location based applications on current Smart phones. Smart phone users have to disclose their identity to Content Providers to accesses these location based services. In spite of tremendous benefits offered by these apps, User Privacy is compromised. In this survey, we identify a logical structure of grouping the concepts of location privacy. It has been examined the location based services from a broad perspective involving definitions, characteristics, devices, applications and an overview of modeling regarding privacy preserving techniques and privacy metrics. It is concluded that the user privacy is addressed in existing applications and analyzed the factors that assess the efficiency of these privacy techniques under real-world conditions. It further helps researchers to identify open issues in the field of location privacy in LBS.

**Keywords:** Spatial Databases, GIS, Location based services, GPS, Location Sharing

**Introduction**

Location based Apps on Smartphone are pocket Information retrieval system like Yellow pages, Directories or Help lines. These explore location based geo-information to users no matter where they are. The Apps lets users to query the public servers to retrieve their point of interest relative to their location. The server processes the request and sends back the query result to the user (Fig.1). In spite of providing enhanced functionalities, these Location based services opens security and privacy issues. While the user enjoys the service, they pay the penalty of disclosing their private data to these public location based servers.

**Location Based Service (LBS)**

LBS has been defined as any service or application that extends spatial information processing, or GIS capabilities, to end users via the Internet and/or wireless network (Koeppel, 2000). LBSs are information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device. (Virrantaus \textit{et al.} 2001). It is a wireless IP service that uses geographic information to serve a mobile user and act as an application service that exploits the position of a mobile terminal (OGC, 2005). According to New Information and Communication Technologies (NICTS), it is an intersection of GIS, LBS and Internet technologies.

\textsuperscript{*}Author for correspondence
E-mail: priya_balu_2002@yahoo.co.in

**LBS Architecture & Characteristics**

LBS is a four layered architecture namely User Interface Layer, Network Layer, Query Processor Layer, Knowledge Transfer Layer. User Interface Layer is the physical user mobile device which consists of Sensors, Positioning systems which helps in determining the user location by GPS. Network Layer is responsible for transferring the user request to and from the service provider using the communication technology. Query Processor Layer’s role is performed by service provider or application provider and responsible for service
request processing of the user such as nearest gas station, nearest friend etc. Knowledge Base Layer is responsible for maintaining the point of interest database and location information and their functionalities in Fig. 2.

Usually this is maintained by third parties or mapping agencies. The Characteristics of location-based services are Location aware i.e. can automatically detect location & deliver applicable content, Context sensitive (light levels, accelerometer, time of day), User Customizable, Ubiquitous access to diverse sources of information, Social networking and Gaming.

**LBS Devices**

The location determination in wireless devices falls into two categories namely Carrier dependent and Carrier independent. All the wireless devices like smart phones, cell phones, ebook readers, laptops, netbooks, and iPad uses any of these technologies for determining location information. Some of the carrier dependent technologies are like:

*Cell Tower*: Mobile device location is determined by triangulation of signals received by the carriers from the towers. Precision is relatively low.

*GPS*: Handset location is determined by the signals from GPS satellites and can be transmitted to the carrier. This technique produces higher precision locations where only the initial location determination is delayed by 30 seconds.

*A-GPS*: Combination of both Cell tower and GPS to overcome the delay of initial startup process.

Carrier independent technologies are:

*Wi-Fi DB*: Wi-Fi database access points are used to determine location of smart phone.

*Cell Tower DB*: Here a database of Cell tower location is maintained and user location is determined by the lookup in cell tower database.

*GPS Chip*: Mobile user location information is determined by GPS chip in the device independent of the carrier. The popular and latest apps under Location based services are Indoor Location Positioning, Location-Based Notifications, Social Route Planning, Location-Based Emergency Phone Calls, Navigation & Mapping, Location-Based Advertising etc. The different categories of LBS Apps are shown in Figure 3.

**Location Privacy**

Location Privacy is a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others - Duckham and Kulik. It is the ability to prevent other parties from learning one’s current or past location - Beresford and Stajano. According to Weston, it is: *When* – A subject may be more concerned about her current or future location being revealed than locations from the past. *How* – A user may be comfortable if friends can manually request his location, but may not want alerts sent automatically whenever he enters a casino or bar. *Extent* – A user may rather have her location reported as an ambiguous region rather than a precise point.

**Privacy aware LBS**

In LBS users query a public server for nearby points of interest but they may not want to disclose their locations to the service. Sharing private data to un-trusted server results in violation of user privacy. To protect against various privacy threats, several studies have proposed different approaches to protect the user privacy at the cost of query performance and query accuracy. There are currently two approaches to location privacy namely 1) Privacy by Architecture which aims to design for model hiding user identity even an attacker has access to the necessary information and 2) Privacy Policies that are trust-based mechanisms that aim to protect location information and any other collected personal data from accidental disclosure or misuse.

**Anonymity based approaches**

Anonymity is a technique of hiding the user identity. This is classified as Pseudonym and cloaking.
techniques. In pseudonym type of anonymity, an individual identity is made anonymous where as in cloaking approach, user actual location is hided by K-anonymizing spatial region. In a quadtree based algorithm\(^1\) was proposed to guarantee k-anonymous location information through reduction in location resolution. This technique uses a Central Anonymity Server for authenticated user connections. In\(^10\), a peer to peer model is developed for anonymous location based queries. Here 2D location of the user are mapped to 1D space which are indexed by a chord based distributed hash table. This model constructs a k-ASr by randomly choosing k consecutive users including the querying user. The mobile users will form a group from her peers via single hop or multi-hop communication\(^5\). The spatial region formed is enclosed of entire group of peers whose action may be on-demand or pro-active mode. This model has less communication cost and response time. No trusted third party is required. A new casper framework\(^20\) is modeled where user location is preserved that consists of two components location anonymizer and privacy aware query processor. The anonymizer blurs the user location into cloaked spatial region based on user privacy requirements. Mouratis and Yiu\(^17\) proposed a network based anonymization and processing is proposed where NAP relies on global user ordering and bucketization. Low computation cost and high performance technique. Bahi\(^15\) and others reviewed a steganographic approach and proposed to hide identity of the user.

Obfuscation based approaches

Obfuscation is a process of adding noise to the user information with the aim of protecting the user's location privacy. Ardagna \textit{etal}\(^2\) studied about the user location that is preserved by means of applying obfuscation operators individually or in combination. An ID shuffle schema is proposed by Chuang \textit{etal}\(^23\) which is based on local synchronization and independent ID update. Here a Mix Zone is designed where nodes will update their IDs but not application services. Reza Shokri and others\(^30\) studied a collaborative protocol which is designed to maintain privacy where users can exchange the location information they already have to peers without

Fig. 3 — Location based service- Types

- Booyah
- My Town
- TapCity

- MapDing
- Shop kick
- YellowPage
- Socialight

- Around Me
- Geopedia
- Nearest Wiki
- Trover

- Crowdmap
- Glympse
- Guard
- Moby

- BlackBerry Traffic
- MyCar Park
- Waze
- Red Rocket

- Flickr
- Geologi
- Tagwhat
- urbandag

- mrip
- Ask a Nomad
- Compass
- Tripbirds

- Goby
- Yelp
- TaskAve
- Voxora

- Booyah
- My Town
- TapCity

- MapDing
- Shop kick
- YellowPage
- Socialight

- Around Me
- Geopedia
- Nearest Wiki
- Trover

- Crowdmap
- Glympse
- Guard
- Moby

- BlackBerry Traffic
- MyCar Park
- Waze
- Red Rocket

- Flickr
- Geologi
- Tagwhat
- urbandag

- mrip
- Ask a Nomad
- Compass
- Tripbirds

- Goby
- Yelp
- TaskAve
- Voxora
contacting the server. Che and Yang\textsuperscript{4} suggested a dual-active spatial cloaking algorithm for mobile P2P networks is designed in such a way that peers not only actively collect but also actively disseminate location information to others. Rupa and Blough\textsuperscript{31} proposed a framework for obfuscating private information is proposed where collaborative filtering is applied to fields of data.

**PIR based approaches**

Private Information retrieval is a technique that allows user to retrieve a data item from a database while hiding the identity of the item from a database server. This technique was first introduced by Chor in 1995. A fundamental approach based on private information retrieval\textsuperscript{1} to process range and K-nearest neighbor queries where hardware based PIR is proposed and index structures are encrypted. This provides stronger privacy guarantees compared to those of the cloaking and anonymity approaches. A variable-sized cloaking region is constructed which increases the location privacy of the user by Olumofin and others\textsuperscript{22}. No trusted third party is required and computation cost is high. The service provider knows the user cloaked region but not the exact location. Instead of single cloaking region, a variable sized cloaking region if formed by VHC cells which results in greater privacy. The user query is processed by downloading the point of interest in single cell instead of entire contents of cloaking region. David et al\textsuperscript{6} proposes a collaborative protocol among users by means of a cryptographic protocol. Here IDs are either shared or exchange between users. Rupa and Blough\textsuperscript{31} discussed a scalable authentication scheme based on elliptic curve cryptography (ECC) and proposed where it allows any node to transmit an unlimited number of messages without suffering the threshold problem.

**Location Sharing policies/approaches**

Location Sharing is technique of broadcasting your location to other users on the network. The popular location sharing apps are Google’s Latitude, IpoKi, Blip etc where these helps to find friends, chat with them. Other popular apps like Gowalla, now owned by Facebook, is tremendously popular “check-in” service that allows users to create a check-in spot for favorite cafes, museums, interesting street scenes, or just about any location that deserves to be shared. It’s great advertising for businesses, fun for the user and useful for those looking for a good restaurant. Foursquare, another very popular app, allows a user to check in from a city location, and critique everything from the service to the dessert menu. Glympse, a popular smart phone app, allows people to share their real-time location through the phone’s GPS feature. This is a fabulous app for parents who want to track their kids’ short journeys and monitor their safety. User often shares their locations in accessing location based services. In some situations like traffic monitoring systems, users share their location continuously. Gruster and Grunwald\textsuperscript{19} found that most of US working population is identified using approximate home and work locations. Beresford and Stajano\textsuperscript{3} identified all users in continuous location traces by examining where users spent most of their time. Home addresses of most drivers were found by Hoh et al\textsuperscript{32}. Krumm\textsuperscript{16} identified from the GPS traces of vehicles. De Mulder et al\textsuperscript{21} could identify mobile users in a GSM cellular network from pre-existing location profiles by using statistical identification processes. Ma et al\textsuperscript{18} studied the erosion of privacy caused by published anonymous mobility traces and show that an adversary can rapidly relate location samples to published anonymous traces.

Durr et al\textsuperscript{6} studied the private user positions which are split into shares of limited precision and distributed among servers of multiple providers. Hence a compromised server only reveals position information of strictly limited precision. TISSA\textsuperscript{32} is proposed where user can choose their privacy modes on location based Apps. They can control the personal information accessed by the applications. The various privacy preserving techniques are evaluated based on parameters such as Trusting third party, Anonymity, No. of users, computational overhead, communication cost and response time. The results are as shown in Table 1. The anonymization requires a third party to trust on. The obfuscation techniques partially confuse the server in locating users and PIR based methods increases computational cost.

**Privacy metrics**

Quantifying location privacy is not yet standardized. It is measured as the accuracy of user location prediction by an attacker. Location privacy\textsuperscript{13} is quantified as expected error in distance between a person’s true location and an attacker’s uncertain estimates of that location. Duckham and Kulik\textsuperscript{8} studied the user location which is distributed at different levels in occupying the coordinates. Here a single query is wrapped by different coordinate
locations to confuse the attacker. Privacy is quantified in terms of entropy where an attacker uses behavioral probabilities in changing pseudonyms. Hoh etal studied the duration over which an attacker could track a subject is quantified as privacy. It measures how long it will take for an attacker to become confused about a subject’s track as the subject seeks to obfuscate his or her location by omitting measured samples. Quality of service generally decreases with increasing location privacy, and researchers seek methods of keeping both at a high level.

Conclusion

In this paper, it has been examined the definition, characteristics, devices and applications of Location based services. Several studies on Location privacy are analyzed and efficiency of these techniques in preserving privacy is summarized. Location sharing policies and quantifying privacy are two areas which needs research attention to standardize. This paper further opens research ideas related to privacy in location based services.

References

16 Krumm J. Inference attacks on location tracks. PERVERSA’07 Proceed of the 5th inter conf Pervasive comput, 127-143 (2007).
24 Priya Iyer K B & Shanthi V, Goal Directed Relative Skyline Queries in Time Dependent Road Networks,. *IJDMS, 4(2)*, April 2012.
26 Priya Iyer K B & Shanthi V, Intelligent Field Finder for goal directed queries in Road Networks, *Proceed of MNCApps, AIEEE(Bangalore,India) August 2012.*
27 Priya Iyer K B & Shanthi V, Spatial Boolean Skyline Boundary Queries in Road Networks, *Proceed of ICCN(Coimbatore, India), July 2012, India*. In press.
29 Priya Iyer K B & Shanthi V, Location based Disaster Management System through Smart phones, *Proceed of ACCT(Visakhapatnam, India), July 2012, India.*