Design and Determination of Feasible Centroid for Meeting from Multiple Geo-Points: A Review

Nikhita Jambhule¹, Jagdish Pimple²

¹M.Tech. Scholar, Department of Computer Science & Engineering NIT, Nagpur, India
²Assistant Professor, Department of Computer Science & Engineering NIT, Nagpur, India

Abstract: In recent years smart phone are become most important gadget for maintaining the daily activities and it also used by maximum population worldwide. Use of smart mapping technology is also increasing in large area like transportations, defense, sports, etc. Mapping applications are always depend upon current detection or preferred location of user or the group. Many application trying to get the user location to serve better service to location based services to user. Sharing location among the group is better solution to know the individuals location. Finding or locating the location at known area or the known cities are usable and also feasible but at unknown location using these services may be risky or not feasible. Considering the above condition, if any group wants to arrange a meeting at location which suits all the members hence it will always better to find centroid of the polygon generated by user geo-locations. It also has issue with finding better options of meeting while calculation.

Keywords: mapping, polygon algorithm, GCM code, Google API, centroid calculation.

1. Introduction

With the development of the ubiquitous wireless technology and mobile positioning technologies and there is explosive growth of location-based services (LBS) in recent years [1]. Mobile clients can issue queries together with their accurate location information and query contents to request LBS. However, the privacy of user's location and query content information may be threatened by the untrustworthy servers. The disclosure of user's location information and query contents are possible to lead to the disclosure of users' behavior patterns, health status, physical stalking, and personal privacy information [1].

Most query tracking models usually consider the background knowledge of the attack on temporal dimension, which means that the attacker has users' information at different moments of cloaking regions. The characteristics of the query attacks for continuous queries in mobile LBS, formalized the attacker's background knowledge in both horizontal spatial dimension and vertical temporal dimension [1]. The concept of privacy is very important for making the communication in WSN secure. Privacy can be defined as- the guarantee that information, in its general sense, is observable or decipherable by only those who are intentionally meant to observe or decipher it. The privacy threats that exist for sensor networks may be categorized broadly into content privacy and context privacy threats [2].

Radio Frequency Identification (RFID) is an automatic identification, non-contact technology that uses radio signals to identify, sort, track and detect a variety of objects including vehicles, goods, people and assets without the need for direct contact. RFID has an appropriate range and is easy to carry [5]. Given the flexibility and convenience of RFID systems, they can be leveraged to detect users’ location information. Meanwhile, users start using location sharing services (LSSs) (e.g. Google Latitude, FireEagle) for updating their location status online social sites, seeing their friends’ locations on a map and identifying nearby friends [5].

2. Related Work

Wei Li, Wei Jiao, Guangye Li[1], proposed Location-Based Service (LBS) combined with mobile devices and internet become more and more popular and are widely used in intelligent logistics, traffic navigation and the point of interest query. However most users be concerned about their privacy when using the LBS because they should provide
their accurate location and query content to the untrustworthy server.

This system analyses the query association attack model for the continuous query in mobile LBS, formalized the attacker’s background knowledge in both horizontal spatial dimension and vertical temporal dimension. In the temporal dimension, the relevance of anonymous space generated by a user in the valid query period and in the spatial dimension, the relevance of different anonymous spaces generated at the same period is compared.

3. Algorithm Goal

In order to cope with query association attack effectively, the shared cloaking region should have k-sharing characteristics. Not only the anonymous space of the user query set meets the m-invariant model, but also the anonymous space is allowed to be shared by its users. That is, it satisfies the characteristics of k-sharing.

Definition: (K-sharing) K-sharing means that a cloaked spatial region not only contains at least k users, and the region is also shared by at least k of these users.

Theorem: If the cloaking region R satisfies the above characteristics, assume the maximum value of k user setting the main database.

In order to prove meeting sharing among different users in the past. LocSafe is comprised in three parts: RFID Tags, social service provider and LE Collectors. We use RFID technology to detect encounters and use attribute-based encryption and broadcast encryption to establish trust and protect users privacy. We evaluate LocSafe by an study of “missed-connections” problems and analysis of system implementation.

The system integrates a GSM Modem which will receive SMS containing the location information and displays it on the Google Map applications. The graphical location information is hosted on a website so that it can be accessed remotely through the internet. The capability of such a system is shown through three working functions that can display the latest vehicle location, route history and route planner. The remote vehicle tracking system corroborations the feasibility of real-time tracking of vehicles which can be used for many applications including vehicle security and fleet managements.

Igor Bilogrevic, MurtuzaJaddiwalla, VishakJoneja, kubra Kalka, Jean-Pierre Hubaux and ImadAad[3], proposed privacy-preserving algorithms for determining an optimal meeting location for a group of users. They perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches.

Wei Xin, Cong Tang, TaoYang, Huiping Sun, Zhong Chen [5], proposed LocSafe method, a “missed-connections” service is used which grants based on RFID technology, in order to prove meeting sharing among different users in the past. LocSafe is comprised in three parts: RFID Tags, social service provider and LE Collectors. We use RFID technology to detect encounters and use attribute-based encryption and broadcast encryption to establish trust and protect users privacy. We evaluate LocSafe by an study of “missed-connections” problems and analysis of system implementation.

they accurate location and query content to the
The degree of privacy of WSN is analyzed using entropy based method. The privacy threats that exist for sensor networks may be categorized broadly into content privacy and context privacy threats [6]. Content privacy threats arise due to the ability of the adversary to observe and manipulate the exact content of packets being sent over the sensor network. In contrast to content-oriented privacy, the issue of context privacy is concerned with protecting the context associated with the sampling and transmission of sensed data.
Sheng Zhong, Li (Erran) Li, Yanbin Grace Liu, Yang Richard Yang[7], proposed privacy-preserving location based services for the three components involved in providing location-based services is the location-based service component, the localization component and the communications component. The focus of our study is on the location-based service component, but we also take the other two components into consideration. This system designed for a novel protocol for a user to control which entities can have access to her location information stored at an untrusted location server. Novel protocols use to provide location-based services which do not require a user to trust a third party.

4. Conclusion

In this paper, short survey of different method is presented. Through which some are finding the location and some method are used for the privacy purpose. In this paper, we have discussed mainly two method one is LBS and another is RFID. This two method are used to the location finding among the different user and preserve the privacy.

References