International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

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

Nikhita Jambhule[1], Jagdish Pimple[2]

[1]M.Tech. Scholar, Department of Computer Science & Engineering NIT, Nagpur, India

[2]Assistant 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].

The WSN cluster based source location privacy scheme for WSN which hides the actual identity of a source node during communication through anonymization [2]. Remote vehicle tracking systems have been available in the market for some time. Their performance is commendable and they can track the vehicle's locations in real time [2].

Determining a suitable location for a set of users is a relevant issues several providers already over variants of this service either as on-line web applications or as stand-alone applications for mobile devices [3]. Not only is such a feature desirable, but it also optimizes the trade-o- between convenience and cost for the involved parties [3].Combined technological advances in location sensing, mobile computing and wireless communication are opening up new and exciting opportunities in the domain of location-aware computing [4].However, there are still some shortcomings that can be addressed to improve the current systems. Firstly, the users often face difficulties in accessing and viewing their vehicle's location in a user friendly graphical interface and secondly, the subscription cost to maintain their active operation can be prohibitive. Thirdly, these system is not easily customizable. For that propose and build a working prototype of a remote vehicle tracking system that can overcome all the issues. That system integrated with Google Map to ease users in viewing and locating their vehicle whenever and wherever as long as there is an internet connection (remotely accessible).

Radio Frequency Identification (RFID) is an automatic identification, non-contact technology that you 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 Loc ation-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 is K, then the attackers adopt query association.

Algorithm design

// Location Distribution awake to Cloaking Algorithm
Input t: time value the cloaking region needs to satisfy;
R: user's query request set
Output: Anonymous space collection
1 L=HilbertOrder(R);
2 for(all l ∈ L){
3 P =P ∪ {l}: S =P ∪ {l.s} ;
4 IS= IS ∪getInvariantSet(l); m=getMaxM();
5 if(|IS ∪ S |≥ m ||((m ≤ p.size)&&(IS==null))){
6 peerGroups = split(P);
7 if(peerGroups!=null){
8 peerGroups.serviceSet = S;
9 annoResult.add(peerGroups);
10 for(all p ∈P){
11 if(Is==null) p.invSet=S;
12 else p.invSet= IS ∩ S ;
13 }//end if
14 remove P from l; P=null; S=null; IS=null;
15 }//end if
16 }//end if
17 }//end for
18 return annoResult;

Muhammad Ridhwan Ahmad Fuad and Micheal Drieberg[2],presents the development of the remote vehicle tracking system which integrates the Global System for Mobile Communications (GSM) Modem and Google Map. The GSM modem will receive the coordinates at the control center through Short Message Service (SMS) and updates the main database.

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 corroboration the feasibility of real-time tracking of vehicles which can be used for many applications including vehicle security and fleet managements.

Igor Bilogrevic, MurtuzaJadliwala, 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 grantees 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.

RFID Tag: People carry RFID tags during daily activities. In LocSafe, every user has a unique RFID tag.

Social Service Provider: A social service provider is a central server to aid in friend locator applications and post-encounter matching of the data that LE Collectors uploaded.

LE Collector: LE Collectors are comprise of RFID readers which are deployed publicly in Common missed connection locations. LE Collectors periodically collect the location and encounter information and upload it to the social service provider.

Aparna Gurjar, A R Bhagat Patil[6], proposed source location privacy scheme for WSN through cluster based anonymization. The system hides the real node identities during communication, by replacing them with arbitrary identities generated by the cluster heads.The simulation results show that the scheme improves the degree of privacy compared to a method which does not have any provision of anonymity for sensor nodes.

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

[1] Wei Li, Wei Jiao, Guangye Li, "A Location Privacy Preserving Algorithm for Mobile LBS. Proceeding of IEEE CCIS2012.
[2] Muhammad Ridhwan Ahmad Fuad and Micheal Drieberg, "Remote Vehicle Tracking System Using GSM Modem and Google Map.IEEE Conference on sustainable utilization and Development in Engineering and Technology.
[3] Igor Bilogrevic, MurtuzaJadliwala, VishakJoneja, kubra Kalka, Jean-Pierre Hubaux and ImadAad, " Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices". IEEE Transaction on Information Forensics and Security, vol.9, no.7, JULY 2014.
[4] Matt Duckham & Lars Kulik**,** "Location privacy and location-aware Computing" survey paper University of Melbourne, Australia.
[5] Wei Xin, Cong Tang, TaoYang, Huiping Sun, Zhong Chen, "Towards Privacy-Preserving RFID-Based Location–Based Services". 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012)
[6] Aparna Gurjar, A R Bhagat Patil, "Cluster based Anonymization for Source Location Privacy in Wireless Sensor Network". International Conference On communication System and network Technology2013.
[7] Sheng Zhong, Li (Erran) Li, Yanbin Grace Liu, Yang Richard Yang, " Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks". Survey paper.
[8] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux "Secure distance-based localization in the presence of cheating beacon nodes," IEEE Trans. Mobile Comput., vol. 9, no. 6, pp. 810–823, Jun. 2010.
[9] G. Chen, H. Bai, L. Shou, K. Chen, and Y. Gao, "Ups: Efficient Privacy Protection in Personalized Web Search," Proc. 34th Int' ACM SIGIR Conf. Research and Development in Information, pp. 615-624, 2011.
[10] Lidan Shou, He Bai, Ke Chen, and Gang Chen, "Supporting Privacy Protection in Personalized. Web Search". IEEE Transactions On Knowledge and Data Engineering, Vol. 26, No. 2, February 2014.
[11] Na Li, Nan Zhang, Sajal K. Das and Bhavani Thuraisingham,"Privacy preservation in wireless sensor networks: A state-ofthe-art survey" Ad Hoc Networks 7 (2009) 1501–1514.
[12] Wei L, Guangye L, Chunlei L. Query-Aware Anonymization in Location-based Service. The 7thInternational Conference on Computational Intelligence and Security(CIS2011), 2011:741-745.
[13] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. 25th IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2005.