

A SURVEY ON PROVIDING LOCATION PRIVACY PROTECTION

G.Saravanan¹, R.Sanjay², G.Sundaramurthy³ and R.Geetha⁴

^{1,2,3} UG Scholar, Department of Computer Science and Engineering, S.A Engineering College, Chennai, India

⁴ Associate Professor Department of Computer Science and Engineering, S.A Engineering College, Chennai, India

Abstract: Location-Based Services (LBS) is used to identify the current location of the user and the user is able to search the point of interest such as hotels, parks which is located near to him. Many of the systems are still using GPS to search any location which does not have privacy. We have surveyed many papers which are related to location privacy. The systems which are proposed earlier have some drawbacks on privacy. The proposed system provides privacy by using Dynamic Grid System (DGS). DGS provides continuous connection with the base station and whenever the user request to find location by querying he has to reveal his current location to the base station. To find the nearby Point Of Interest (POI) the K-Nearest Neighbour algorithm is used. K-Nearest Neighbour provides the user required POI even if the user is on the move. The system uses semi-trusted third party which is known as Query Server (QS) which do not collect and store any information of the user.

Key words- Location-Based Services, Dynamic Grid System, Query Server, Point Of Interest, K-Nearest Neighbour.

I. INTRODUCTION

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link[]. The main concept involves two phases known as mobile communication and mobile hardware as shown in Figure 1. In current situation of web network, many individuals utilize area based administrations to get data in view of their present area from different specialist organizations. At the point when client look for any close-by area, then it gives data to the untrusted specialist organizations. For client area protection benefits there are a few strategies have been proposed as of late.

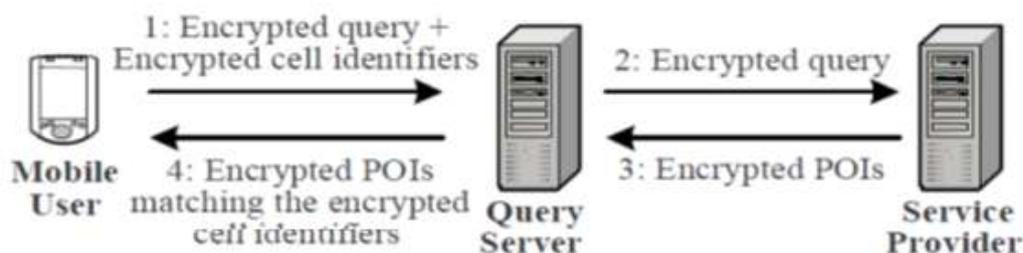


Figure 1 :System Architecture of DGS

The first strategy is the fully trusted outsider. In the middle of the client and specialist co-operation there ought to be a trusted outsider which is known as QS and it is utilized to conceal the client's area from the specialist co-operation. The principle point of outsider is to track the present area of client and conceal the client's area into a shrouded range. This trusted outsider has a few disadvantages. All clients as often as possible overhaul their present area to the base station, despite

the fact that they don't get to the area based administrations. Attackers know the correct area of the clients, if the outsider has the client's area data. The second strategy is Private data recovery or careless exchange. This venture proposes a client characterized protection matrix framework called dynamic network framework, dynamic lattice framework is utilized to give security safeguarding depiction and consistent area based administrations. The point is to put a question server in the middle of the client and specialist co-op which is semi trusted outsider.

II. RELATED WORK

Nardine Basta, Amal El-Nahas, et.al [1] expressed that mobile opportunistic networks are interconnected with each other, the data packets are delivered among multiple mobile devices through opportunistic communication. Network portioning, long delays must be handled by mobile opportunistic networks. To make any decision in mobile opportunistic networks, it uses social based approach which was developed recently. This research work uses several new geo social metrics which provides location information and social relationship between users. For mobile opportunistic networks there are several routing algorithms exists to achieve stable routing.

Bin Guo, Zhu Wang et.al [2] conveyed that Mobile Crowd Sensing and Computing is used for cross space and large scale sensing as well as enhance both user contributed data in online and participatory sensory data in offline. It also explores complimentary roles and fusion, collaboration of machines and crowd sensing. This paper develops a framework for developing human in the loop mobile crowd sensing and computing.

Xing Su, Hanghang Tong, et.al[3] demonstrated about the usage of smartphones are increasing in day to day life for every people, which is used to recognise the user motion activity by accepting the input as raw sensor reading. It is used in high-impact applications such as health, personal bio-metric signature and urban computing and also provides advanced activity recognition.

Yu Wang, Fan Li, et.al [4] expressed that there are different topologies proposed for underlying network topologies which is used to achieve the communication without delay and it guarantees the delivery of packets using specific routing approaches. However, most of the topologies are using two-dimensional networks but in practice the networks are deployed with three-dimensional networks. This work extends 2D into 3D geometric topology. In 3D networks the properties like bounded degree, constant power stretch factor are efficient than in 2D networks.

Balk Hoh, Marc Gruteser [5] proposed a system that maintains high data accuracy, they get the results from analysing a set of GPS tracking vehicles which does not provide privacy for users in low density areas and does not meet the privacy requirements. To overcome this some criterion is used which provides privacy.

Toby Xu, Ying Cal, et.al [6] conveyed that mysterious area data might be associated with confined spaces, for example, home and office for subject re-distinguishing proof. This makes it an extraordinary test to give area security assurance for client area based administrations. The system which was already developed, receives conventional K-secrecy and guarantees that every area uncovered in administration solicitations in a spatial area that has been gone by at least K clients. This technique requires a client to determine a proper esteem of K clients to accomplish a higher level of protection security. This is dangerous on the grounds that security is about feeling, also, it is ungainly for one to scale the user's inclination utilizing a number. In this paper, they developed an inclination based protection show. The model permits a client to express her security necessity by determining an open area, which the client would feel good if the area is accounted to the client.

G.Srinivasan, A.Latha, et.al [7] expressed about the current years, look has been expanded towards remote sensor arrange in different fields. It comprises of a huge number of little and minimal effort sensors with constrained power, calculation and correspondence abilities. The hubs have restricted beginning measures of vitality that is expended in various rates relying upon the power level and the planned collector. Vitality protection and scalability are presumably two most basic issues in planning conventions for multi-hop remote systems. The conventions produced for these systems ought to be proficient and furthermore adaptable. Topographical directing calculations are

known to be adaptable however their productivity has never been relatively examined. In land directing calculation, the data packets are sent by a hub to its neighbour in light of their individual vitality. They demonstrated a calculation named Localized Energy-Aware Restricted Neighbourhood directing (LEARN) which discovers course for any source and goal matches asymptotically and ensure the vitality effectiveness of its course on the off chance that it finds the course effectively.

Yu Wang, Dingbang Xu, et.al [8] demonstrates that the spatial shrouding strategies are used to accomplish area protection in area based administrations. In the majority of the current spatial shrouding strategies, the completely trusted outsiders have been utilized and it is required between the client and specialist co-operation. The area anonymizer which is known as completely trusted outsider is utilized to conceal the client's present area into a shrouded range when a client associated with area based administrations and this needs to fulfil K-anonymity by including in any event K-1 different clients. This approach finds the shrouding range in view of number of clients to take care of the customized protection necessity issue. These methods depend on the k-anonymity protection necessity and accomplished local area security, despite the fact that spatial shrouding systems are connected in distributed situations. On the off chance that the clients are trusted with each other then they can share their area amongst themselves and shroud the area data to different companions. There are some circulated techniques which were already there and they do not require the client to be trusted with each other however it utilizes various Trusted Third gathering. Incremental closest neighbour queries are utilized as a part of numerous calculations, where the present area of the client contrasts from the stay area which is brought up by the inquiry and if question is fulfilled then many purpose of intrigue will be appeared to the client. Without the utilization of trusted outsider the suitable area of the client can be known, which comes about just in local security.

Jing Yuan, Yu Zheng, et.al [9] demonstrated that GPS-prepared taxicabs can be viewed as portable sensors probing traffic on street surfaces, and cab drivers are typically experienced in finding the speediest (fastest) course to a destination in view of their insight. In this paper, they mine savvy driving bearings from the verifiable GPS trajectories of a substantial number of taxicabs, and furnish a client with the for all intents and purposes speediest course to a given goal at a given departure time. They proposed a period subordinate historic point chart, where a hub (milestone) is a street fragment much of the time navigated by taxicabs, to display the insight of cabbies and the properties of element street systems. At that point, a Variance-Entropy-Based Clustering methodology is devised to gauge the circulation of travel time between two points of interest in different schedule openings. In view of this diagram, they outline a two-arrange steering calculation to figure the practically speediest course. They assembled the framework in light of a genuine world direction dataset created by more than 33,000 cabs in a time of 3 months, and assess the framework by leading both engineered tests and in-the-held assessments. As an outcome, 70% of the courses proposed by this strategy are quicker than the contending strategies, and 20% of the courses have similar outcomes. By and large, half of our courses are no less than 20% quicker than the contending approaches.

Marco Gruteser, Dirk Grunwald, et.al [10] expressed the propels in detecting and following innovation empower area based applications however they likewise make huge security dangers. Obscurity can give a high degree of security, spare administration clients from managing specialist organizations' security arrangements, and diminish the administration suppliers' necessities for shielding private data. It may ensure unknown utilization of area based administrations which require the exact area data transmitted by a client and this can't be effectively utilized to re-distinguish the subject. This system shows how to design middleware and calculations are utilized and brought together. The versatile calculations change the determination of area data along spatial or fleeting measurements to meet indicated namelessness imperatives in light of the elements who may be utilizing area benefits inside a given territory. Utilizing a model in view of car activity checks and cartographic material, they appraise the practically anticipated spatial determination for various secrecy imperatives. The middle determination created by their calculations is 125 meters.

Thomas Brink Hoff, et.al [11] expressed that benchmarking spatial temporal database frameworks requires the meaning of appropriate datasets recreating the commonplace conduct of moving objects. Past methodologies are used for producing spatial temporal information which doesn't consider the moving items regularly of the given system. Along these lines, benchmarks require datasets comprising of such "system based" moving objects. In this paper, the most imperative properties of system based moving objects are introduced and talked about. Basic viewpoints are the most extreme speed and the greatest limit of associations, the impact of other moving objects on the speed and the course of a question, the sufficient assurance of the begin and goal of a question, the impact of outer occasions, and time-planned movement.

The summary of the survey has been listed in Table 1

Table 1: Summary of the survey

Reference	Computat ion cost	Privacy	Cloaking area	Communicati on cost	GPS connectivity
T-Drive:Driving Directions Based on Taxi Trajectories	Very high	low	low	Very high	Yes
Preserving privacy in GPS traces via uncertainty aware path cloaking	high	Medium	low	High	Yes
Feeling-based Location Privacy Protection for Location-based Services	medium	medium	medium	Medium	Yes
providing Location-Aware Location Privacy Protection for Mobile	medium	medium	high	Medium	Yes
Proposed System	low	high	high	Low	No

III. ENHANCED PRIVACY MODEL

As our system gives much importance for privacy, the dynamic grid system is used and it allows the user to continuously connect with base station.

The Query server which is known as semi-trusted third party is used to provide the link between service provider and user and it will not collect, store the location information of the user. It is used as an intermediate between the user and service provider because the information is passed through this.

In the existing system the third party server unveil the information which is sent by the user and it insert the wrong message and unwanted information, whereas our proposed system uses QS which does not unveil the user information, insert any wrong and unwanted information.

The main idea of DGS is to determine the approximate location which is known as query area of the user, so the user is able to say that he/she within the area the DGS specified. The query area which is specified by the DGS is divided into equal-sized cells, it is based on the dynamic grid structure specified by the user. The query area which is specified by DGS is encrypted along with the grid cell's identity to obtain encrypted identifier.

If the user queries to find any location, the query includes two phases. They are encrypted query and identifiers which is passed through QS. When the query reaches base station it decrypts the query, then process the query and encrypts the required information by the user which is sent through QS. Now the user decrypts the information which is sent by base station. By this way the privacy is achieved in our proposed system as shown in figure 2.

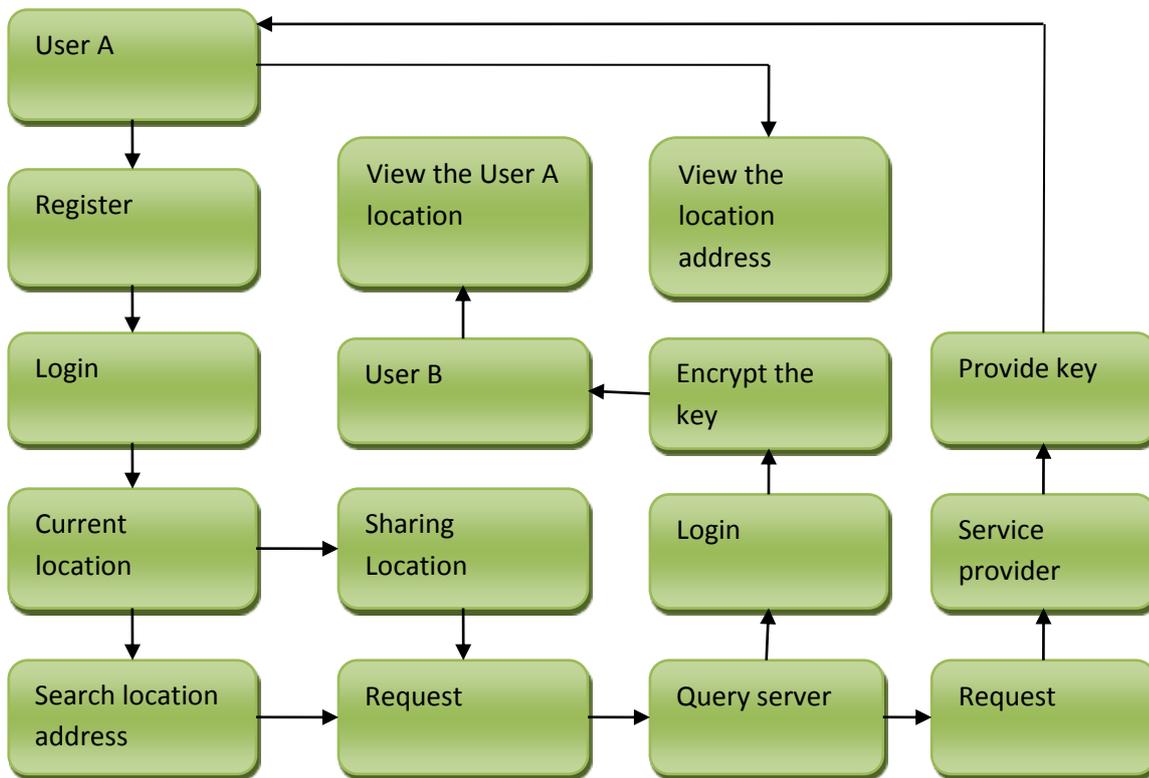


Figure 2: Work Flow Diagram

K-Nearest Neighbour algorithm is used in our system. As the algorithm stated earlier, it provides the POI required by the user even if the user is on the move. Here, the base station receives the query requested by the user then decrypts it and then it encrypts the user required information which is sent to user through QS. Then the user decrypts and view the information provided by base station. The encryption and decryption takes place by using the keys.

IV. CONCLUSION

To evaluate the performance of DGS, we compare it to the state-of-the-art technique requiring a TTP. DGS provides better privacy guarantees than the TTP scheme, and the experimental results show that DGS is more efficient than the TTP scheme, in terms of communication cost. DGS always outperforms the TTP scheme for NN queries; it is comparable or slightly more expensive than the TTP scheme for range queries. We proposed dynamic grid system for providing privacy-preserving continuous Location based service. Dynamic grid system does not require any fully-trusted third party instead we require only the much weaker assumption of no collusion between Query server and Service. The efficient protocols have been designed for our Dynamic grid system

to support both continuous k-nearest-neighbor and range queries. To evaluate the performance of Dynamic grid system. Dynamic grid system provides better privacy guarantees than the trusted third party scheme.

REFERENCES

- [1] Nardine Basta, Amal El-nahas, Hans-Peter Grossmann, and Slim Abdennadher, “Geo-social mobility model for vanet simulation,” *Journal of Mobile Multimedia*, Vol. 10, No. 1&2 (2014) 107–127.
- [2] Bin Guo, Zhu Wang, Zhiwen Yu, Yu Wang, Neil Y. Yen, Runhe Huang, Xingshe Zhou, “Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm” *Journal ACM Computing Surveys* volume 48 Issue 1, September 2015.
- [3] Xing Su, Hanghang Tong, “Activity Recognition with Smartphone Sensors”, *Journal IEEE*, June 2014
- [4] Yu Wang, Fan Li, “Energy-efficient topology control for three-dimensional sensor networks”, *International Journal of Sensor Networks*(2008) in *ACM Volume 4 Issue 1/2*, July 2008
- [5] Balk Hoh, Marc Gruteser, “Preserving privacy in GPS traces via uncertainty aware path cloaking”, *14th ACM conference on Computer and communications security*, 2007
- [6] Toby Xu, Ying Cai, “Feeling-based Location Privacy Protection for Location-based Services” *Proceedings of the 16th ACM conference on Computer and communications security* Pages 348-357, November 09-13 2009.
- [7] T. Xu and Y. Cai, “Location anonymity in continuous location-based services,” *Journal ACM GIS*, 2007.
- [8] Yu Wang, Dingbang Xu, “providing Location-Aware Location Privacy Protection for Mobile Location-Based Services, *IEEE*, Volume 21, Number 3, June 2016
- [9] Jing Yuan, Yu Zheng, Chengyang Zhang, Wenlei Xie, Xing Xie, Guangzhong, “ T-Drive: Driving Directions Based on Taxi Trajectories”, *IEEE Transactions on Knowledge and Data Engineering* Volume: 25, Issue: 1, Jan. 2013.
- [10] Marco Gruteser and Dirk Grunwald, “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking” *ACM 1st international conference on systems, applications and services*, page 31-42.
- [11] Thomas Brink Hoff, “A Framework for Generating Network-Based Moving Objects”, *Springer* Volume 6, Issue 2, June 2002.