A Novel Approach for Query Processing In Location Based Services

Srikanth. R
Department of Computer Science and Engg,
National Institute of Technology Hamirpur (H.P.)
ravula_srikanth@yahoo.co.in

L. K. Awasthi
Department of Computer Science and Engg,
National Institute of Technology Hamirpur (H.P.)
lalit@nitham.ac.in

***Abstract*—The emerging trends in the location-detection devices together with ubiquitous connectivity have enabled a large variety of location- based services (LBS). Location-based services are becoming popular service used by the mobile users. The mobile users' location plays a key role to provide service in LBS, but it other side it is grievous dimension of their privacy, so it necessary to keep the user information anonymous to the other parties. The important issue in LBS is to achieve accurate service result queried by the user, hence it is important to use the mobile user accurate location. Using the location accurately raises some concerns on behalf of the user's privacy. Traditional solution for meeting these requirements is by using the means of a anonymizer. Anonymizer uses K-anonymity cloaking technique to hide the user location this technique is called K- anonymzing spatial region (K-ASR). Traditional method needs complex query processing algorithms at the server side and have drawback of tracking user mobility. In this paper we have proposed a new model for mobile users to retrieve the result quickly, accurately and increases user's privacy. The proposed system continuously evaluates the query issued by the user.**

***Keywords*— Location based services (LBS), Privacy, K-Anonymizing spatial region (K-ASR), Anonymizer**

I. INTRODUCTION

Nowadays, location-detection devices —such as cellular phones, GPS-like devices and RFID, etc—are more and more widely used. These location-detection devices together with ubiquitous connectivity have enabled a large variety of location-based services (LBS) which are able to tailor services according to the location of the user requiring the services. LBS can be used in a variety of contexts [6], such as health, work, personal life, etc. LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games.

There are several reasons that explain the great popularity of LBS in the research community[8], of these one of the main research area in LBS is privacy of the user. Unfortunately, LBS may threaten our privacy. Malicious attacker may collude with LBS provider to steal users' location information and query logs [1].

Generally LBS services mainly rely on *k*-nearest-neighbor queries (*k*NN), which retrieve *k* points-of-interest (POIs) closest to the user's location. *K*-anonymity has been widely studied to protect privacy in LBS. Its main idea is to make the user issuing the query indistinguishable from at least *K*-1 other users. Most existing works [1][2][3][5], adopt the framework shown in Fig.1. The user sends its location, query and *K* (no. of results) to the anonymizer, which is a trusted third party. The anonymizer cloaks the exact user location to *K*-anonymizing spatial region (K-ASR) including at least *K*-1other users. Then the anonymizer sends the *K*-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymizer. At last, the anonymizer calculates the results which is more appropriate to user and sends them back to the user. Two serious drawbacks of this framework are: 1) high processing cost since the LBS server has to process range *k*-nearest-neighbor queries [1], and 2) high communication cost since the number of candidate results can be large.

Different from *K*-anonymity is SpaceTwist query processing [4] technique which sends a false location to the server instead of a cloaked region. SpaceTwist requires only simple query processing algorithm on the server—namely, incremental nearest neighbor (INN) retrieval. However, SpaceTwist may fail if the attacker already knows the locations of all the users. According to [4], the location of the user issuing the query can be bounded in a region Ω. If only one user lies in the region Ω, then attacker can easily infer that the query is issued by the user, which may threaten the user's privacy. The reason why SpaceTwist may fail is that it does not guarantee *K*-anonymity.

So far in the area of the LBS lot of research has been done in the privacy issues of the stationary LBS[11,12], there is only small research in the field of the mobile client (eg Client moving from one city to other city) who dynamically moves from one cell network to other cell network randomly while moving to the destination[7,9]. This is the main motivation for the work on this paper.

In this paper, our work has been being described as follow:

- We propose a new framework to protect privacy in LBS. In this model we protect privacy and user traceability attack in LBS.

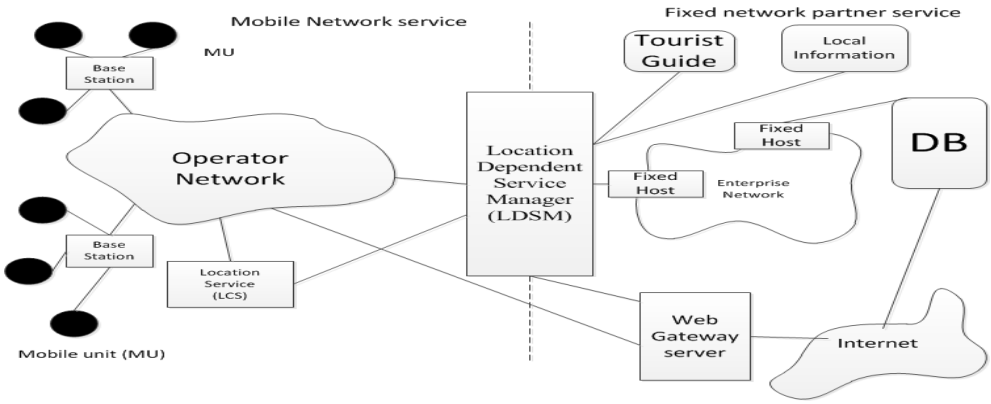

Fig-1: General architecture of the Location based service

II. RELATED WORK

In our methodology, we draw upon work done in the areas of both cryptography and location-based services. In this section, we briefly describe related work in these areas.

A. Location-based services

In the peer-to-peer model of LBS, there would be a group of clients or peers who want to mutually compute some location-related function in the absence of a centralized trusted third party server. One of the common queries in this model are aggregate nearest neighbor or group nearest neighbor queries where the "nearest neighbors" are points of interest in the vicinity such as restaurants, hospitals, gas stations, etc. So a typical group nearest neighbor query for a group of peers would be "Which is the restaurant that is closest to all of us" or "Find a meeting spot that is within 2 miles of all of us?"

Figure-1, represents the general architecture of LBS. The left part of the figure is Mobile Network service which is connected by wireless network this part is responsible for collecting query from mobile users (MU). Location dependent service manager (LDSM) acts as the middle ware to the Mobile network service and service provider. The right part of the figure is the service provider which is connected by wired network.

Some of the general work in this direction (non-privacy preserving) includes, among others. One of the widely referenced works in this area is SpaceTwist [4] which is a protocol where a querying client asks the LBS server to return a set of *k* points closest to its own location or *k-N*earest neighbors. The authors do not apply their protocol to the group nearest neighbor problem which is quite different from *k*-nearest neighbor and has a different set of privacy requirements. There has been quite some work in the area of aggregate nearest neighbor queries which show how to do query processing of aggregate nearest neighbor queries in road networks.

B. Traditional K-anonymity

Most existing works on LBSs adopt *K*-anonymity by using the framework illustrated in Fig. 2. This framework works as follows: A user sends its location, query ID of the user and cloaks the exact user location to *K*-ASR including at least *K*-1

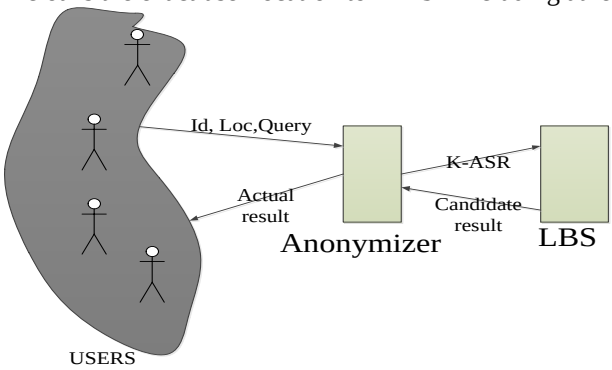

Fig-2: Architecture of traditional K- Anonymity

other users. Then anonymizer sends the *K*-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymizer. At last, the anonymizer which knows the locations of all the users calculates the actual results and sends them back to the user. There are two drawbacks of this framework: 1) high processing cost at the server side since the LBS server has to process range *k*-nearest-neighbor queries, and 2) high communication cost since the number of candidate results can be large.

C. Public-Key Cryptography

One drawback of a private-key (traditional cryptography) system is that it requires the prior communication of the key K between Alice and Bob, using a secure channel, before any ciphertext is transmitted. In practice, this may be very difficult to achieve.

The figure-3, describes the public key cryptography system. The idea behind a public-key system is that it might be possible to find a cryptosystem where it is computationally infeasible to determine. If so, then the encryption rule could be made public by publishing it in a directory (hence the term public-key system). The advantage of a public-key system is

that Alice (or anyone else) can send an encrypted message to Bob (without the prior communication of a secret key) by using the public encryption rule. Bob will be the only person that can decrypt the cipher text, using his secret decryption rule.

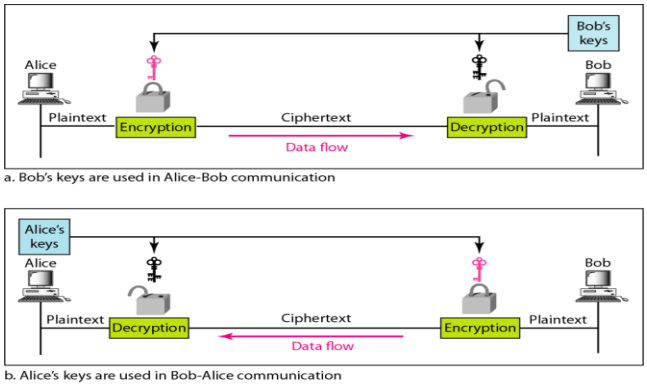

Fig-3 Description of the public-key system

Cryptographic techniques first used in LBS service is demonstrated in [10].

III. SYSTEM DESCRIPTION

In this paper we have proposed a new technique to process LBS query for mobile users, who frequently change their position. Earlier system's as described in section 2 Traditional k- Anonymity uses a single server and multiple anonymizers, hence the workload of the server increases and traceability of the users is increased as there is only server preserve track of all the mobility of the user. To overcome these issues we have developed a new system as described in following paragraph.

System environment:

In the proposed system environment, we have considered the base station (BS) as LBS server. The BS which basically serves the Voice and data communication can also simultaneously serve as the LBS application server, by using BS station as the LBS server there is no need of setting up another environment for handling the LBS application. Distribution of the LBS server in various cells is shown in the figure- 5(a).

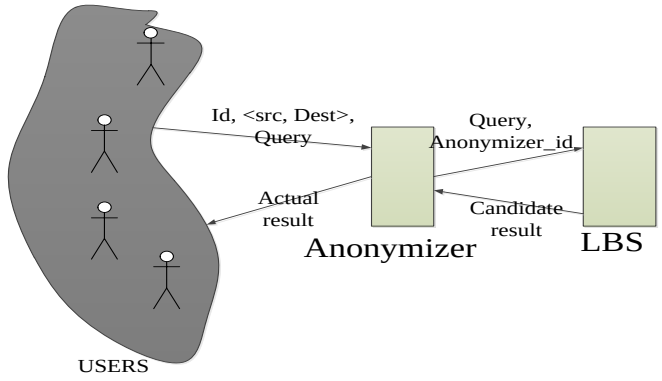

Fig-4: Architecture of proposed model

Each LBS server will be storing the Point of interest data such as shopping malls, petrol pump, and all information that normal user queries in location based service this information is restricted to particular area of the server which it is covering.

The proposed architecture of the system is as shown in the figure 4, proposed system is divided into three categories here we have a user, anonymizer and server. In this system we have also distributed anonymizers according to the areas as shown in the figure 5(b). We have distributed anonymizer into area and theses anonymizers can receive the data and sense its local environment of user mobility at the regular interval and update the required information to the server/user depending on the situation. The location of the user is updated in two process, the two process are as follow one way is when a phone call arrives/ dialed by the user his location is updated and the other process is update of user location by the help of the anonymizer.

The proposed environment of the both LBS server and anonymizer is as shown in the figure- 5(c).

Proposed model:

The proposed system is as shown in figure 4, we have a group of mobile users who issues the LBS query, these user frequently change their position as per their requirements. Mobile user system has the CA (coordinate Agent) , QA(Query Agent). CA is used to get the current time, Location of user Loc (Long, Lati.). QA is used to collect the information of the query and other relevant information of the query.

The proposed model is illustrated as shown in the algorithm described below:

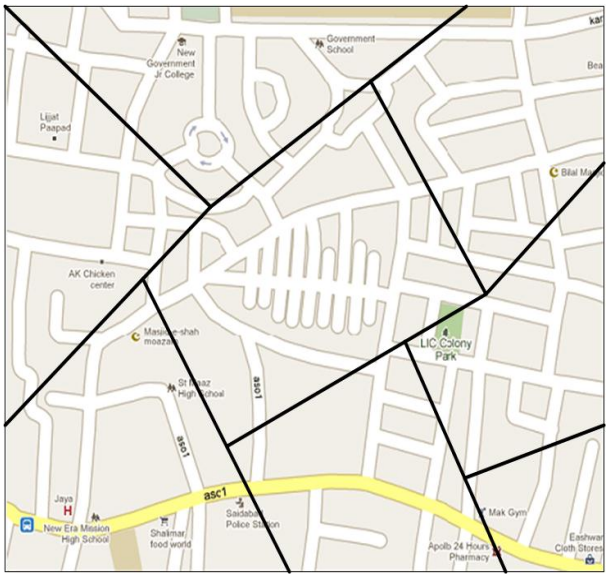

Fig-5(a) Deployment of LBS server over a geo-graphical Area

1. Mobile user (MU), issues the query and public key to the nearby anonymizer, Anonymizer passes the query and key to the base station (BS). As the LBS server is deployed at the BS, LBS processes the query and returns the result back to the BS

2. By step-1, the BS knows that the user is in its region and gives a active signal to all the anonymizers in that particular region.
3. Anonymizers Senses its nearby location and if MU is present in its region then that Anonymizer informs the information the BS by this step BS knows the exact user location.

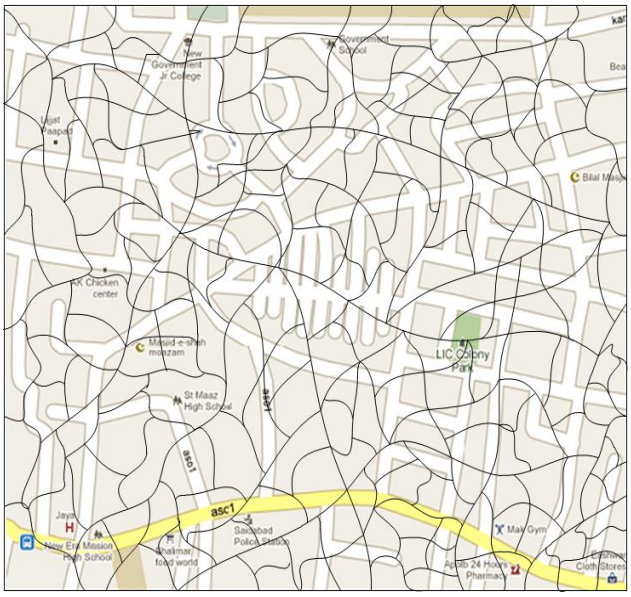

Fig-5(b). : Geo-graphical space division based on Anonymizers

4. If Anonymizer senses the MU in its region it first checks the local database for the query result otherwise forwards the query information to the BS that is followed in the step-3

The proposed system is as shown in figure 4, we have a group of mobile users who issues the LBS query. Mobile user system has the CA (coordinate Agent), QA (Query Agent). CA is used to get the current time, Location of user Loc (Long, Lati.). QA is used to collect the information of the query and other relevant information of the query.

Query issued by the mobile users include the following information:

1. id – Mobile user id who issues the query
2. Query – Query depends on the location
3. Public key of the Mobile user

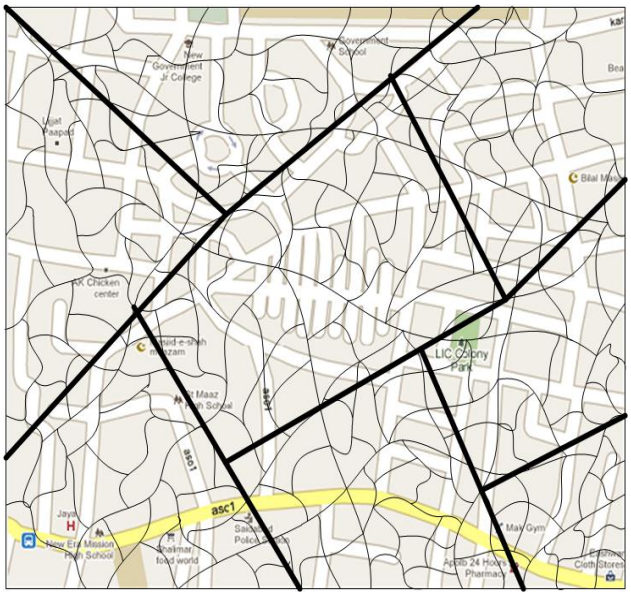

Fig-5(c). : Geo- graphical area division based on both Anonymizer and LBS server

Above information is delivered to the anonymizer by encrypting with the public key of the Anonymizer, so that information delivered to the Anonymizer is confidential and secure. Anonymizer stores the above information in the database. Anonymizer forward's the above query information to the server. Above information is delivered to the sever by encrypting with the public key of the server. Server opens the information using its private key. At the server side the query is processed by the server, and returns the result back to the anonymizer. Server knows the information of the anonymizer so it encrypts with the Anonymizer public key and forward the result Anonymizer. It forwards the result to the desired user based on the id by encrypting the result by user's public key.

Public_key_of _user	Location__user_last_found		Time_ of_issue _Query	Source	Destination	Query	Query_result
	Longitude	Latitude					
1A122-3343f-….			10:30:45	ABC	ASD		
2de67-16281-….			10:35:00	CDE	QWE		
: :	: :	: :	: :	: :	: :	: :	: :
45452-45df2-….			11:45:42	DFG	ZXC		

Table-1: Database at the anonymizer

IV. SUMMARY

This paper has mainly focused on user privacy for mobile users in LBs environment. Proposed system performs better than other system since our system uses new model for query processing and is not based on K-ASR so drawbacks of K-ASR have been eliminated and moreover the user path tracking attack has been overcome since the server doesn't store the information regarding user and his activities. Server load in the proposed system is very low since here we had deployed many servers which store information only regarding that particular area and can only process that small area than compared to existing system which store information regarding large geographical area. Our model illustrate that the query processing costs of our proposed system are lower than those of TKA, KAWCR, Space Twist because in our model the database of the whole region is stored in a place there is no need to split the query based on the dependencies of various databases.

	Proposed System	**KAWCR**	**TKA**	**Space Twist**
User Privacy	High	Medium	Low	Medium
Storage at Anonymizer	Medium	Medium	Medium	Medium
Query processing cost	Low	High	High	Medium
Communication cost	Low	Low	High	High
Server load	Medium	Medium	High	High
Traceability attack	Low	Medium	High	Medium

Table-2: Analysis of various query processing system

The only drawback our system is requirement of storage capacity at the anonymizer is high than compare to the previous model.

V CONCLUSION

In this paper, we propose a new framework to protect privacy in location-based services for the mobile users. Proposed system has better security and has strong defense system from the attack of the attacker. The main strength of the system is that the system gives accurate result quickly and does not store the information about users who has accessed the system so that if intruder hacks the system he does not get any information regarding user and his identity. In this paper we had seen that the proposed system have better performance than compared to the earlier existing system. In future we would like to work on the minimization of the server load, so that the failure rate of system can be minimized.

References

[1] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries." In *IEEE TKDE*, 2007.

[2] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Priv´e: Anonymous location-based queries in distributed mobile systems," In *WWW*, 2007.

[3] C. Zhang and Y. Huang, "Cloaking Locations for Anonymous Location Based Services: A Hybrid Approach," In *GeoInformatica*, Vol.3, No.2, pp.159-182, 2009.

[4] M. L. Yiu, C. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services," In *ICDE*, 2008.

[5] T. Wang and L. Liu, "Privacy-aware mobile services over road networks." In VLDB, 2009.

[6] Gartner, "Gartner Identifies the Top 10 Consumer Mobile Applications for 2012"

http://www.gartner.com/it/page.jsp?id=1230413, April 2010.

[7] Yiming Wang; Lingyu Wang; Fung, B.C.M. ,"Preserving Privacy for Location-Based Services

with Continuous Queries," ICC '09. IEEE, Page(s): 1 – 5, 2009.

[8]Tabassum, K.; Hijab, M.; Damodaram, A.," Location dependent Query Processing – Issues, Challenges and Applications," Computer and Network Technology (ICCNT), Page(s): 239 – 243,2010.

[9]Xiaolan Yin; Zhiming Ding; Jing Li, "Moving Continuous K Nearest Neighbor Queries in Spatial Network Databases," Page(s): 535 – 541, 2009.

[10] Yan Huang; Vishwanathan, R. ,"Privacy Preserving Group Nearest Neighbour Queries in Location-Based Services Using Cryptographic Techniques ," 2010 IEEE Global Telecommunications Conference , Page(s): 1 – 5, 2010

[11] Mohamed F. Mokbel, Chi-Yin Chow, Walid G. Aref , "The New Casper: Query Processing for Location Services
without Compromising Privacy ," Page(s): 763- 774, 2006

[12] Xiaopeng Xiong, Mohamed F. Mokbel , Walid G. Aref "SEA-CNN: Scalable Processing of Continuous K-Nearest Neighbor Queries in Spatio-temporal Databases, " ,2005