Providing Location-based Assistance for Subscribers with Highly Secured Network Structure

Hari Haran M Shetty
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Mohammed Fuzail Sharieff
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Priyanka K K
Engineering Student
Department of ISE
AMC Engineering College, Bangalore.

Vidya Rao
Assistant Professor
Department of ISE
AMC Engineering College, Bangalore.

***Abstract*-The Location-Based assistance(LBA) provides the subscriber to get their location continuously to an untrusted server to get their services required according to their location which leads to privacy risks.But the problem with the existing system is that the LBA technique has few disadvantages it does not provide partially reliable third party, it provides restricted privacy and incurring high communication. This paper proposes asubscriber security structureknown as highly secured network structure (HSNS) the initial integrated system accomplish four requirement for security -preserving snap print and regular location privacy is approved (i) This system needs a partially reliable simple matching operations perfectly. (ii) Protected snapshot and continuous location privacy is approved under supported models.(iii) Depending on the subscriber's requirements the communication cost will be estimated not on the subscriber's privacy level. (iv) Using the uniform functions and algorithms of the system it is possible to support the other spatial queries of the subscriber search area located in the similar space regions.**

Keywords*: *Highly Secured network structure, Location security, Location-based services, Space-temporal query processing, Cryptanalysis.

I.INTRODUCTION

In today's world there is an increasing growth of Internet connectivity where people use for Location based services to get the required information of the current locations collected by different service networks. The search operation depends on the subscriber's point of interest (POIs). It is possible to construct a profile of the subscriber depending upon their interests by tracking their records.

There are number of techniques introduced for subscriber's privacy location using LBS. In common these techniques has been divided into two groups and they are (I) it is been completelysecured into three units. (II) Private information retrieval (PIR). The main advantage of completely secured unit is that it is been placed in between the subscriber and the service network which helps to hide.

The subscriber information from the service network and also keeps the track of the perfect location of all subscriber's queries. In the PIR technique it does not actually need a third party but it needs high connection between subscriber and the service networks.

In this paper we introduce a subscriber defined privacy grid system known as dynamic grid system (HSNS)which provides privacy for the continuous location and snapshot. The main point is that it is been located in a partly secured into a three unit structurenamed as query server (QP) which is been placed in between the subscriber and the service provider(SP).The main control of QS is to be just a semi- trusted party where it will not be able to collect or store any of the subscriber's location information. The actual meaning of partially reliable party is that the query server will determine the location of the subscriber it will perform the perfect matching of the location it does not modify or drop the messages and it does not create any messages.

The HSNS system considers the following points: (i) there is no TTP required. Our system only needs a partially - reliable query server which has to be placed in between the subscribers and service networks. (ii) It provides a secure location privacy where it does not provide the subscriber's location to any other subscriber. (iii) There is a low communication cost where it does not depends upon the area used by the subscriber queries but it just depends upon the point of interest required for the search area. (iv) It is capable of HSNS wiring number of spatial queries using the same system without changing any of the functions and algorithms.

A . PRESENT STRUCTURE

The Spatial cloaking approaches has been largely used to save subscriber venue privacy in LBS. all of the present spatial cloaking approaches depend on a completely – reliable third party, usually termed location anonymizer which is needed in between the subscriber and service provider. When the subscriber subscribes to Location Based Service, the venue anonymizer will blur the subscriber's correct location into a cloaked area so that the cloaked area will have at least k – 1 different subscribers to satisfy k-anonymity. But a system with similar location privacy it’s highly difficult for the subscriber to specify personalized privacy requirements. Then feelings based technique alleviates the issue by finding a cloaked area depending on the number of its visitors that is as popular as the subscriber’s required public region. But spatial clocking approaches can be applied to peer-to-peer environments, these approaches rely on the k-anonymity privacy requirement and only achieve regional location privacy. Further, these approaches requires subscribers to depend each other, as they have to show their venues to other peers and rely on other peers’ venue to blur their locations, another different method was released that does not require subscribers to depend on each other, but it uses multiple TTPs.

Other family of algorithms uses incrementing nearest neighbor queries, later the query begins at an “anchor” venue that is different from the real location of a subscriber and alternatively receives higher points of interest till the query is successful.

II. RELATED WORK

A framework for supporting anonymous location-based queries in mobile information delivery systems. B. Bamba *et al.,*[1] has discussed about the highly secured network security under three conditions. It provides a location privacy protection preference profile model, called location P3P, which allows mobile subscribers to explicitly define their preferred location privacy requirements in terms of both location hiding measures and location service quality measures. Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment.

Last but not the least, secured network incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization.Enabling private continuous queries for revealed subscriber locations have discussed by M. F. Mokbel *et al.,[2]* has proposed a new robust spatial cloaking technique for snapshot and continuous location-based queries that clearly distinguishes between location privacy and query privacy achieve. It has two main goals: (i) supporting private location-based services to those customers with public locations, and (ii) performing spatial cloaking on-demand basis only (i.e., when issuing queries) rather than exhaustively cloaking every single location update.

Protecting location privacy with personalized anonymity using the architecture and algorithms which was been proposed by the B. Gedik *et al.,*[3] they have described a scalable architecture for protecting the location privacy from various privacy threats resulting from uncontrolled usage of LBSs. This architecture includes the development of a personalized location anonymization model and a suite of location perturbation algorithms. A unique characteristic of the location privacy architecture is the use of a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. The framework enables each mobile client to specify the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to accept when requesting k-anonymity-preserving LBSs.

Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking M. Gruteser et al.,[4] has done this related work on this paper presents a middleware architecture and algorithms that can be used by a centralized location broker service. The adaptive algorithms adjust the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints based on the entities who may be using location services within a given area. Using a model based on automotive traffic counts and cartographic material, we estimate the realistically expected spatial resolution for different anonymity constraints. The median resolution generated by the algorithms is 125 meters. Thus, anonymous location-based requests for urban areas would have the same accuracy currently needed for E-911 services this would provide sufficient resolution for way finding, automated bus routing services and similar location-dependent services.

Preventing location-based identity inference in anonymous spatial queries was worked by

P. Kalnis*et al.,*[5] it present a framework for preventing location-based identity inference of subscribers who issue spatial queries to location- based service They propose the HSNS formations based on the well-established K-anonymity concept to compute exact HSNS for range and nearest neighbor search, without revealing the query source. Our methods optimize the entire process of anonymzing the requests and processing the HSNS formed spatial queries.

III. BACKGROUND

Our HSNS supports k- NN challenges and security continuation active collection. The area is organized in which it views the description of the HSNS for processing the active collection of challenges and addition of supporting their explanations. The challenges of the operator initially provides a query range in which the operator is convenient to disclose the information that the person is located somewhere within that query range. The query range is expected to be a rectangular range defined by the equivalent for the bottom left-hand tip (xa,ya) and the top right-hand tip (xt,yt).Attention that the operator is not required to be at the center of the query range because the location can be anywhere in the range.

So our structure can also provide irregular space regions consider an example where the border of a town or a nation it can be in a least border rectangle range according to the model the irregular space region provides a squared area. The query range is been divided into a m × m equal-sized network cells to build a active network structure, where the m is an operator.

Our HSNS has two main levels for security-continuation active area query processing. The first level finds an initial HSNS were for a range query, and the second level additionally controls the query HSNS were based on the operator required location updatesa regular area of queries is described by keeping the track of the point of interest within a operator detailed distance. The area of the operator present location will be (xu,yu) for a certain time period.

IV HIGHLY SECURED NETWORK STRUCTURE

In this portion we explain the highly secured network structure for regular range area of query and the k-NN queries. Our HSNS has mainly two stages which will discover the first response for the range area query and secondly it will maintain the query response depending on the subscribe location information.

In common the regular range area query is discussed by using the protocol step.

Highly secured network structure (by the subscriber) the proposal of this step is to build a highly secured network structure in detail required by the subscriber. The query range is assumed it will be in the rectangular area which is been represented by the vertex of bottom-left vertex and the top-right vertex. The each grid cell of the network structure can be obtained by:

$$(c,r) = \left(\left\lfloor \frac{x_c - x_b}{(x_t - x_b)/m} \right\rfloor, \left\lfloor \frac{y_c - y_b}{(y_t - y_b)/m} \right\rfloor\right)$$

Where each of the grid of the query range area will be processed and calculated according to the subscribe required information.

V NEW CHALLENGES

The new proposed concept introduced in this paper is to provide location based assistance for subscriber with highly secured network structure.

The concept is to add a partially reliable third party, appellate query server (QS), between the subscriber and the service provider (SP).The QS only needs to be partially reliable. Because it will not collect/store or even have access to any subscriber's location information. Partially reliable in this situation HSNS that when QS will try to catch the venue of the subscriber, it still properlydoes the normal matching operations required in the protocol, i.e., it won't reform or develop new messages. An unreliable QS will randomly modify and drop messages as well as introduce fake messages, for that reason our system depends on a partially reliable QS.

The concept of highly secured network structure (HSNS). In HSNS, a querying subscriber first determines a query area, where the subscriber is able to show the fact that he is at someplace within this query area. Later the query area is split into same-sized grid cells based on the secured network structure specified by the subscriber. Later, the subscriber encrypts a query that has thedata of the query area and the secured network structure, and encrypts the particularity of each grid cell intersecting the required search area of the spatial query to generate a set of encrypted identifiers (I) the encrypted query and (II) the encrypted identifiers to Query Server, which is a partially reliable party located between the subscriber and service provider. Query Server stores the encrypted identifiers and onwards the encrypted query to Service Provider specified by the subscriber.

A. *Advantages of New Challenges*

Then each selected POI, Service Provider encrypts its information, with the help of secured network structure specified by the subscriber to locate a grid cell closing the POI, and encrypts the cell identity to create then encrypted identifier for that POI.
The encrypted POIs with encrypted identifiers are returned to Query Server. Query Server contains the set of encrypted POIs and only returns to the subscriber a subset of encrypted POIs identifiers matches encrypted identifiers initially sent by the subscriber. Later the subscriber receive the encrypted POIs, then decrypts toobtain their perfect location and computes query forHSNS answer.

VI SYSTEM ANALYSIS

A. Service providers (SP): structure supports number of service providers. Each *Service Provider is* a spatial database management system which will stores the venue information of a particular type of *static* POIs, hotels or bar, or the store information of a certain organization, such as polar bear or kfc. The spatial database uses an existing spatial index

The system architecture of our highly secured network structure (HSNS) is designed to provide privacy-preserving continuous LBS for mobile subscribers. Our structure has three important integrals, service providers, query servers and mobile subscribers

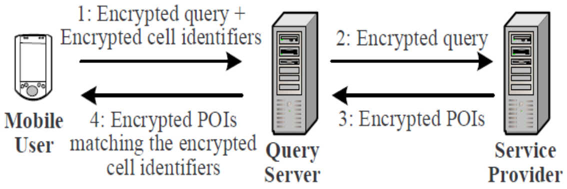

Fig 6 System Architecture of our HSNS

We will describe the main entities and their interactions, and then present the two spatial queries, i.e., range and k-nearest-neighbor (NN) queries, supported by our structure or secured structure) to index POIs and HSNSwere range queries (i.e., retrieve the POIs located in a certain area). As depicted in Fig.6.1, *Service Provider*does not communicate with mobile subscribers directly, but it provides services for them indirectly through the query server (*QS*).

B. Mobile subscribers*:* Each mobile subscriber is equipped with a Global Positioning Services enabled device that determines the subscriber's location in the form (x_u,y_u). The subscriber can acquire snapshot or continuous LBS from our structure by issuing a spatial query to a particular *Service Provider*through *Query Server*. Our system helps the subscriber prefer a query area for the spatial query, such that the subscriber is willing to reveal to *Service Provider*the fact that the subscriber is located in the given area. Then, a secured structure is developed and is embedded in to an encrypted query that is on warded to *Service Provider*, it will not disclose any information about the query area to *Query Server*itself. In addition, the communication cost for the subscriber in HSNS will not be based on the query area size. This is one of the main features that distinguishes HSNS from the present techniques based on the fully-reliable mediator.

When referring into query area for a query, the subscriber will generally examine many factors. (1) The subscriber specifies a minimum privacy. For a Photostat spatial query, the query area will be in the lesser interment rectangle of the city in where the subscriber is present. If better privacy is required, the subscriber can select the required level as the wanted privacy level. The size of the query does not depend no performance implications whatsever on the subscriber, and a subscriber can freely select the query area to suit the subscriber for his own requirements. For continuous spatial queries, subscriber again first select a query area showing the lesser privacy level wanted, but also takes into consideration possible movement within the time period *t* for the query. If displacement at the extreme legal speed could lead the subscriber other than of the lesser privacy level query area inside the query time *n*, subscriber enhances the query area correspondingly.

A bigger query area does have an impact on Query Serverand Service Provider inmeans of workload and cost of communication, but the structure is assumed to be in between the subscriber and Query Server, and the load on this link and on the subscriber will not reston the query area size. A structure parameter can be defined to reduce the higher query area size returned to a subscriber, acceptable not maximum limit of the client-side application.

C. Query servers (QS)**:**partially reliable party placed in between the mobile subscriber and *Service Provider*. Same as the most known infrastructure in existing privacy-preserving techniques for Location Based Service, *Query Server*can be sustained by a telecom subscriber .The control data flows of our HSNS are as follows:

i. The mobile subscriber sends a request that will have (a) the identity of a subscriber-specified Service Provider, (b) an encrypted query (which includes information about the subscriber-defined secured network structure), and (c) a set of encrypted identifiers (which are calculated based on the subscriber-defined secured network structure) to Query Server.

ii. Query Serverwill have the encrypted identifiers and on warded the encrypted query to the subscriber-specified Service Provider.

iii. Service Providerdecrypts the query and meets a correct set of POIs from its database. It later encrypts the POIs and their corresponding identifiers depends on the secured network structure specified by the subscriber and forwards them to Query Server.

iv. Query ServerReturns to the subscriber all the encrypted POI whose encrypted identifier matches anyone of the encrypted identifiers first sent by the subscriber. The subscriber decrypts the arrived POIs to build a candidate HSNSwere set, and then completes a simple filtering activity to prune false positives to compute a perfect query HSNS.

That there is a secured channel between the subscriber and Query Server. This suspicion is required as Service Providerwill be able to understand the subscriber's location if it can eavesdrop on the communication between the subscriber and Query Server. The securedchannel can be easily be established with normalizing methods such as identity-based encryption. Then also note that the data privacy of Service Provideris preserved with respect to Query Server, as Query Serveronly obtains encrypted information about the POIs, and client can onlydecrypt the POIs.Query ServerHence does not learn any information about the POIs.

VII. EXPERIMENTAL RESULTS

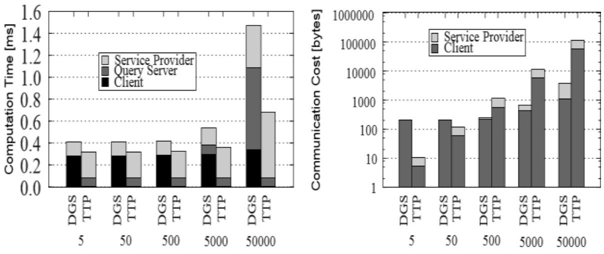

Fig 7. Performance metrics

Estimate the performance of our HSNS for both continuing range and *K*-NN queries with simulations.Deployed a continuous spatial cloaking scheme using the fully-reliable third partymodel. TTP relies on a fully-reliable location anonymizer, that is placed in between the subscriber and the service provider (*SP*), to blur a querying subscriber's venue into a cloaked area that has the querying subscriber and a set of K− 1 other subscribers to satisfy the subscriber specified K anonymity privacy requirement. To safeguard the subscriber's continuing venue privacy, the locationgoes on changing the cloaked area to store the querying subscriber and the K− 1 subscribers. A privacy-known query processor at Service Providerreplaces a set of POIs to the querying subscriber with the location anonymizer.Then, the querying subscriber computes an perfect query HSNS from the candidate POIs. Different tries such as secret informationretrieval or oblivious HSNSare fundamentally different and put a much more burden in terms of complexity of the computation on the subscriber's side. They also compare unwanted against TTP and our HSNS in means of communication bandwidth required, making the similarity between TTP and HSNS the most equivalent one.

VIII CONCLUSION

The Proposed Highly Secured Network Structure (HSNS) is used for providing security preserving regular location services. The HSNS contains the challenge attendant and then it has a package source and it also has cryptanalysis process where it splits the complete query processing test is been collected and then it is been split into two forms which is been executed individually by the query server and the service provider. The HSNS which does not involve any of the completely secured third units rather it needs only the weaker idea where there is no involvement between the query server and service provider. It is been disturbed and also leads the transport the information to carry and it can be away from the subscribe to the inexpensive and high-bandwidth link between query server and service provider. It also been constructed for the efficient protocols where it supports both regular k-nearest-neighbor (KNN) and the area queries. For the evaluation of the performance of the HSNS it is been compare it to the state-of-the-art approach requiring a trusted third party.

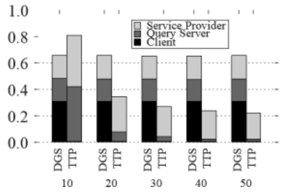

Fig 1.Comparison of HSNS with TTP

The HSNS provides better security which guarantees that the trusted third party arrangement and the experimental results that shows the HSNS is the order of magnitude more efficient than the trusted third party are any in particular with communication rate. The conditions of the computation cost where the HSNS also always out performs the trusted third party arrangement for KNN queries it is comparable or may be slightly more costly than the trusted third party arrangement for the area demands.

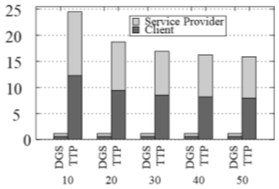

Fig 2. Comparison of HSNS with TTP

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, “Supporting anonymous location queries in mobile environments with PrivacyGrid,” in *WWW*, 2014.

[2] C.-Y. Chow and M. F. Mokbel, “Enabling private continuous queries for revealed subscriber locations,” in *SSTD*, 2014.

[3] B. Gedik and L. Liu, “Protecting location privacy with personalized k-anonymity: Architecture and algorithms,” *IEEE TMC*, vol. 7, no. 1, pp. 1–18, 2015.

[4] M.Gruteser and D. Grunwald, “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking,” in *ACM MobiSys*, 2014.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” *IEEE TKDE*, vol. 19, no. 12, pp. 1719–1733, 2013.

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: Query processing for location services without compromising privacy,” in *VLDB*, 2013.

[7] T. Xu and Y. Cai, “Location anonymity in continuous location-based services,” in *ACM GIS*, 2014.

[8] “Exploring historical location data for anonymity preservation in location-based services,” in *IEEE INFOCOM*, 2014.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: Anonymizers are not necessary,” in *ACM SIGMOD*, 2010.

[10] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, “Efficient oblivious augmented maps: Location-based services with a payment broker,” in *PET*, 2011.