International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Special Issue 2; March 2018; Page No. 31-36

An efficient algorithm for privacy in nearest Neighbourhood search in MQMO for point clouds

Phaltane Anjali D, Vidya Jagtap
Department of Computer Engineering, GH Raisoni College of Engineering Chas, Ahmednagar, Maharashtra, India

Abstract
Due to the growth in mobile phones, the location based service (LBS) market is growing tremendously fast. Many mobile phone applications uses LBS such as store finder, car navigation system etc. LBS provide services to mobile users based on location & data profile of user's hence users private information may get violated. In order to protect users private information many solutions are offered but most of them only addressed on snapshot query and no support for continual query and Moving Query Moving Object (MQMO). This paper focuses on MQMO & also protects users' private information using PIR. In this paper we proposed a system to reduce the communication cost in client-server architecture as an object needs to report its location to the server only when it leaves its safe region or server sends location update request. Hilbert transform is used to find shortest path to reach destination & protection of user data. Voronoi diagram is used for space partitioning and cell binding. Also we describe a motion adaptive indexing scheme for indexing the database of moving continuous query. The concept of motion sensitive bounding boxes (MSBs) is used in order to model moving objects & moving queries.

Keywords: LBS, PIR, MQMO, MCQ, MSBs, Hilbert transform, voronoi diagram

1. Introduction

Location based services is a certain service that is offered to the users based on their locations. There are many LBS such as location based traffic report, location based store finder, location based advertisement etc. But these location based services uses location information of user as well as user's private data, because location based services rely on the implicit assumption that users agree on revealing their private user information.

Location based services trade their services with privacy i.e. if a user wants to keep her location privacy, she has to turn off her location detection device & temporarily unsubscribe from the service. Several social studies report that users become more aware about their privacy, so the private information of LBS should be protected.

To provide location privacy different methods are used: Location perturbation, Spatial cloaking, Temporal cloaking, Spatial-temporal cloaking & k – anonymity.

For Location privacy also different architectures [4] are used such as: Client server architecture, trusted third party architecture, Peer to peer co-operative architecture. In order toprovide LBS to users it is necessary to find NN. In order to issue a NN-query there are 2 ways: a) Snapshot Query b) Continuous Query [1].

In snapshot query object sends a query requesting nearest POI to the location based service provider. LBS server initiates a response according to each service request.

In continuous query, the object sends a query requesting nearest POI to LBS. Based on this single query request, LBS server updates user/object with nearest object as the object is moving [1].

Most of the paper focuses only on snapshot query & does not consider moving query [2, 3], some paper [4] focus on moving query search in LBS but no security & privacy issues are considered. In order to protect user's private information PIR (private information retrieval) is used that will allow user to retrieve information from a database [2, 5, 6] but only addressed snapshot query.

In this paper we propose a technique which mainly focus on moving query & moving object that will continuously protect user's private information in CNNQ.

In MQMO, the query used as well as object moves within a spatial network. This technique uses [1] Voronoi diagram with Hilbert curve along with R-tree geometric data storage. The R-K-NN [7] is used along with K-NN in order to give accurate NN in MQMO.

Hilbert transform based reverse NN provides better result in terms of time complexity memory consumption & Voronoi (vo) size than existing work.

2. Preliminaries

2.1 Problem Definition

The location based services has become increasingly important in many applications such as position-based services, supply cycle management, travel control, and so on. These applications usually involve queries over spatial networks with continuously changing and problematical travel conditions. There may be possibilities of exposing users private information to the third party servers where the location information about the users will be tracked. The malicious attackers may use the location information about the users. The k nearest neighbor query verification with location points on Voronoi diagram increases the verification cost on mobile clients. The reverse nearest neighbor queries by assigning each object and query with a safe region is applied such that the expensive re- computation is not required as long as the query and objects remain in their respective safe regions Nearest neighbor has few deficiencies in processing query such as1) Highly Dependent on Training data 2) Includes Redundant data 3) Increased Processing time 4) Low speed. The above drawback leads to inefficient query processing.

2.2 Moving Query and Moving Objects

In this paper MQMO means mobile query (user) & moving object (POI). In order to provide privacy and security in CNNQ, the user's private information should not be revealed to any third party as user continuously receives update on nearest POI. The nearest POI in the path of a moving object at each point of a segment as the object moves along the segment is called as CNN.

3. Related Work

In [2], they propose idea that allows user to specify & receive exactly K-NN from LBS with lower transmission cost, minimal user computation & minimal amount of database information disclosed. They propose two algorithms, first one return exact K-NN. They propose 2 techniques in order to provide privacy in LBS:

- Two-tier spatial transformation
- Three-tier spatial transformation
- Cryptographic Transformation

Two tier spatial transformations provide direct communication between user & LBS server. But due to waiting for K-NN there is delay in query processing.

Three tier transformation uses trusted third party anonymizer but it has to depend on honesty of trusted anonymizer & single point of attack.

Cryptographic transformation is based on PIR scheme that allows a user to retrieve information from db without revealing the exact information retrieved but only addresses snapshot query & no support on moving query. In [3], focuses on group nearest neighbor query and also considers the privacy issues of peer to peer model of LBS. In peer to peer model of LBS, all peer's keep their location information private from each other & combine all peer's in group find a common location and work in the absence of a trusted third party. This paper proposes a solution to a problem in previous solution for group nearest neighbor query which required each peer should share its location information with all other peer's in group, in the presence of trusted third party, but here privacy may be violated. This paper provides user privacy in peer to peer network, in absence of trusted third party & if the peers are trusted. For this purpose Secure Function Evaluation (SFE) protocol i.e. Yao's protocol [11] is used in semi honest model. This protocol has 2 variants: a) semi-honest model b) dishonest model. This paper uses Yao's protocol in semi-honest model. In order to answer group nearest neighbor queries in LBS in semi-honest user model, this paper use a methodology which is based on SFE problem and "Garbled Circuit"? Garbled circuit is basically used to give answer to group NN query.

For answering the GNN query, the semi-honest model uses two setting: centralized and distributed. This paper uses a fully distributed setting for secure multi-party group nearest neighbor function evaluation protocol (GNN).

In [7] an energy-efficient search algorithm based on the Hilbert curve (HC) index is developed [7] to support CKNN queries for wireless data broadcast system. Paper focuses on problem of answering CKNN queries in wireless broadcast system. The [7] is based on the assumptions that all the data objects are logically stored in the broadcast server.

In [13] the profile based anonymization model is proposed in [3] which use spatial cloaking. To implement this location is generalized so that at least K-l users should be in spatial-temporal region and at the same time contains at least additional K-l users with identical profile of the user. In [15] user location is replaced by dummy location & issues a query using dummy location but using this approach, nearest point of interest is always approximate not exact.

In [5] some framework does not require trusted third party, since privacy is achieved through cryptographic technique. In order to achieve privacy, PIR technique is used which will protect user's private information. The paper guarantees privacy against correlation attack. It implement exact-NN & approximate-NN algorithm. Though this approach achieves stronger privacy for snapshots queries still LBS releases more information to user & so transmission costly.

In [1] evaluates a technique for protecting privacy in CNNQ in LBS focused on MQSO. They proposed a technique using Voronoi diagram & Hilbert curve order to isolate object & R-tree geometric data storage is used for indexing in db.

Only few of the paper focuses on LBS privacy in MQMO but has certain limitations. We are using some techniques and algorithm that will focus on privacy in LBS in CNNQ with focus on Moving Query and Moving Object. Also we would like to extend our work in the direction of MQMO with focus on motion –adaptive indexing for efficient processing of moving continual queries over moving object. In [1] the query verification problem for k-nearest-neighbor queries over LBS is focused but approaches proposed in this domain verify both the distance and the shortest path to K-NN results simultaneously, a network Voronoi diagram–based verification approach that utilizes the network Voronoi cell of each result object to verify the correctness and completeness of K-NN result is implemented with regard to both distance and path. It does not focus on MQMO and indexing using R*tree increases the no of updates. The k nearest neighbor query verification with location points on Voronoi diagram increases the verification cost on mobile clients. The reverse nearest neighbor queries by assigning each object and query with a safe region is applied such that the expensive re-computation is not required as long as the query and objects remain in their respective safe regions. Also existing system does not work on moving object, which increases the number of updates to the indexes. Nearest neighbor have few deficiencies in processing query such as 1) Highly Dependent on Training data 2) Includes Redundant data 3) Increased Processing time 4) Low speed. The above drawback leads to inefficient query processing. For better result than K-NN we would like to extend our work in the field of privacy in LBS in MQMO by using RK-NN classification algorithm.

4. Drawbacks of Existing System

The existing system uses K-NN for query retrieval process which includes redundant data. The Voronoi diagram is used in the existing work to represent the location information in the graphical format. The K-NN classification algorithm is utilized on the Voronoi diagram for retrieving the location data as per user demand. The user data may get leaked, because of less security in the Voronoi diagram and also the K-NN classification algorithm cannot provide the accurate nearest location information to the users.

N has few deficiencies in processing query such as

1. Highly Dependent on Training data
2. Includes Redundant data
3. Increased Processing time

The above drawback leads to inefficient query processing

5. Proposed System

The key idea of the propose system is to advance the security of the user and to focus on efficient retrieval of solutions. The paper focus on a special kind of data mining called as spatial data mining. Generally when the user is surfing for certain information over the online network, the location information of the user will be stored in the third-party server. As many of the third party server not secured there is possibility of hacking the information by the hacker. Thus information about location of the user gets leaked that leads to several critical problems such as kidnapping the particular individual. In order to provide high level security to user. The information about users can be stored in the Network Voronoi diagram over which Hilbert Transformation is applied to increase security to the user information. In the case of Query Retrieval Process the results retrieved should be clear and complete and should not contain duplicates.

To overcome the drawbacks of existing system, the reverse RK-NN and Hilbert transformation are implemented to provide a solution to the problems.

Step 1: Key Generation / Query Submission

Initially, the keys are generated and distributed over a network. DO obtain a private and a public key through a key distribution center. The private key is confidential and is accessed only by DO, whereas the public key is accessible by all clients. Using its private key, the DO sends the data to SP which is used for query processing. The queries are gathered from the user and based on query the data processing take place on spatial networks and the queries will be then be authenticated by using the RK-NN classification algorithm by getting the details from the neighbors.

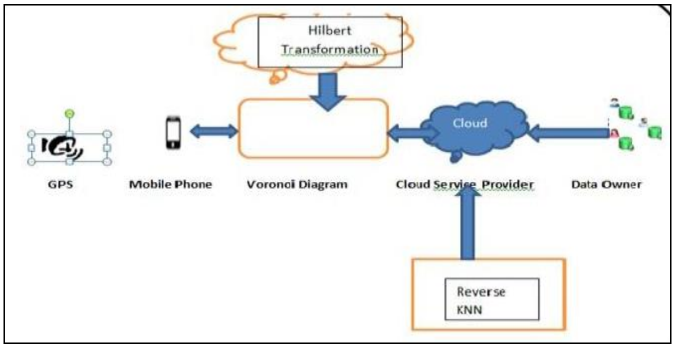

Fig 1: System Architecture

Step 2: Forming the Spatial Network

The creation of users, servers, and the query processor forms the network. The network formation is done by using the java platform. The user is the one who queries to the network for gathering the location information. The server is the one who stores and gives the location based information present in their storage. The server stores the spatial network information in the format of Voronoi diagram. The query processor is the one who gathers the queries from the user and will retrieve the results for those queries from the servers.

The previous technique used for storing the information is the MBR. The MBR represents the objects in form of circular points within the rectangular boundary. The objects are spatially distributed and exact location of the object within the boundary is easily identified, leads to security lacking for the object. The Voronoi diagram on comparing with MBR provides high security by storing the data within an irregular polyhedron structure. The exact location of the object cannot be determined due to unstructedness of the Voronoi. Consider a set of distinct objects say P = p1; p2; pn in a region R, the Voronoi diagram of P, denoted as V D (P), partitions the space of R into t disjoint regions, such that each object pi in P belongs to only one region and every point in that region is closer to pi than to the other objects of P. The region around pi is called the Voronoi polygon or Voronoi cell of pi, denoted as V C(pi).Therefore, the Voronoi diagram of P is union of all Voronoi cells V D (P) = V C(P1); V C(P2):V C(Pt).Voronoi neighbors shares a common edge.

Step 3: Applying Hilbert Transformation over Network Voronoi Diagram

Hilbert curve is a space filling curve that is used only to find shortest path to reach the destination. The continuous research process leads to a solution that by applying the Hilbert curve along with transformation over the Network Voronoi diagram provides high confidentiality to the user. The user data remains protected. Hilbert curve is a specialized curve that is highly complex in this structure that leads to complex index calculation Hilbert transformation is used to store range of values in the curve over the Voronoi diagram. The transformation prevents the unauthorized user from getting the exact value. Thus the security of the user is ensured and thereby preventing the leakage of the highly protected information and in today modern environment security plays important role in different fields'. Security must be ensured in every day today activities of the user.

Step 4: Query Retrieval Process

The process deals with retrieval of results for an input query. The paper focus on spatial mining and it deals with getting spatial data for a spatial query. The existing system uses K-NN (K-Nearest Neighbor) to get K-NN spatial data results for the inputted spatial query.

The proposed system uses RK-NN (Reverse K-Nearest Neighbor) technique for retrieving spatial results for the given spatial query. The bidirectional K-NN (RK-NN) take search to the next level and produces accurate results. The proposed algorithm over comes the drawback of the K-NN.

The advantage of RK-NN includes:

1. Eliminates redundant data.
2. Less processing time.
3. High speed.
4. Less memory consumption.

The proposed system provides better results when compared to the existing system in terms of high security and efficient query retrieval process.

A) Module Description

Module 1: In this phase we create Basic GUI of Mobile client, LBS Server and Service provider, this module consists of basic communication flow of mobile client with LBS, Service provider.

In this module, Service provider will register with LBS server to provide service for mobile user. Service provider willsubmit their data with keys also mobile client will register with LBS to use service of service provider with keys. We also use GPS to show the object in moving state.

Module 2: In this phase we implement Existing system as:

i) Voronoi Diagram: In this module we super-impose Voronoi diagram over area, and then map the area to a grid. All the POI in the area belongs to a cell. The contents of the cell represent the two endpoints of a query line segment. The Voronoi diagram is used in the existing work to represent the location information in the graphical format. The K-NN classification algorithm is utilized on the Voronoi diagram for retrieving the location data as per user demand.

ii) Hilbert Curve: Hilbert curve is a space filling curve that is used only to find shortest path to reach the destination. The continuous research process leads to a solution that by applying the Hilbert curve along with transformation over the Network Voronoi diagram provides high confidentiality to the user. We transform these values which represent set of points in a multi-dimensional space into records in a database akin to. Queries on the records are queries on these sets of points which are now represented by Hilbert values. We use R-tree structure for the geometric data storage.

Module 3: The proposed system uses RK-NN (Reverse K-Nearest Neighbor) technique for retrieving spatial results for the given spatial query. The bidirectional K- NN (RK-NN) take search to the next level and produces accurate results. The proposed algorithm over comes the drawback of the K-NN. In this module, we describe a motion-adaptive indexing (MAI) scheme for efficient processing of moving continual queries over moving objects. It uses the concept of motion-sensitive bounding boxes (MSBs) to model both moving objects and moving queries.

B) Implementation Environment

The possible technologies to implement proposed system:

- Java, J2ME SDK 3.0.
- Glassfish Server to conduct client and server experiments.
- Development of LBS server using JSP and Servlet.
- Mobile Emulators for access for moving queries and moving object.
- Sun Francisco dataset file.

6. Mathematical Modeling

Let S be a System such that, S={S, I_p, e, O_{op}, F}

Where,

Iip ={q, Rk(P), G,Se}

e(partial output)={KNN,R-KNN}

F={VD(),HC(),VO.result()}

A) Problem Statement of Model

Let Se –Search keyword, Rk(P)-Ranked List Provided by Provider, P- items that match the search term in POI db. P={P1, P2, ….., Pn}

B) Voronoi Diagram (VD)

Given: P={P1,P2…..,Pn} in Rk, Voronoi diagram of P is denoted by, VD(P).VD(P)={VC(P1),VC(P2),……VC(Pn))-space partition VD into VC.

Property 1: Given VD(P), NN(q)=P1 iff q∈VC(P1).

Property 2: User should not be uniquely located in that region,there should be atleast k-user.

C) Hilbert K-Annonymizing

All user locations are sorted based on their Hilbert order. To anonymize a user, we compute *start* and *end* values as:

- *start = ranku* - (*ranku* mod *ku*)
- *end = start + ku* – 1.

D) PIR –Protocol

Db={X(x1,x2,…xn): is a n bit string}, Client wants to know value of x1? Client sends Q[E(I)] to server, where E: algorithm used for generating the obfuscated vector.

Server reply with v(x,q). Client compute x1=v(x,q)

Instead of using PIR which replicates the data we are using computational PIR.

E) VKNN= verify k-nn algorithm

Let q be the query point, VO is the verification object, is parameter. H is min-heap which sorts points according to their distances to query q and VO. result () is the kNN result returned by the server. In VCP compute VC();where VC1() is the first object of Voronoi cell, "L[i+1]. location H.pop()",Let (L[i]) is last verified object of Voronoi cell and has not been visited yet, is inserted into the min-heap H.

F) Moving Objects

Moving object is represented by a quadruple Om= {io, p, v, ap} where,

- Io: unique object identifier.
- P (Px, Py): Current position of moving object.
- V= (Vx, Vy): current velocity vector.
- ap: set of properties about the POI.

G) Moving Query

Moving Query is represented by a quadruple Qm= {iq, io, r, f} where,

- iq: is unique query identifier.

- io: is object identifier of focal object of query.
- r: shape of special region bound to focal object of query.

7. Results

The following is the expected result for time complexity of the propose system with the existing system. X-axis contains number of queries and Y-axis contains time in millisecond. The expected result shows that propose system consumes less time.

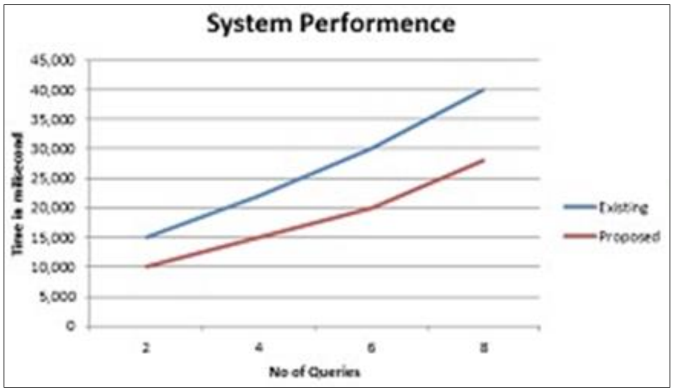

Fig 1

The verification object is authenticating the query sent by the users. The VO means the Voronoi and it is the region where all the information get stored on the server. The size of the Voronoi increases the security and reduces the intrusion of the data.

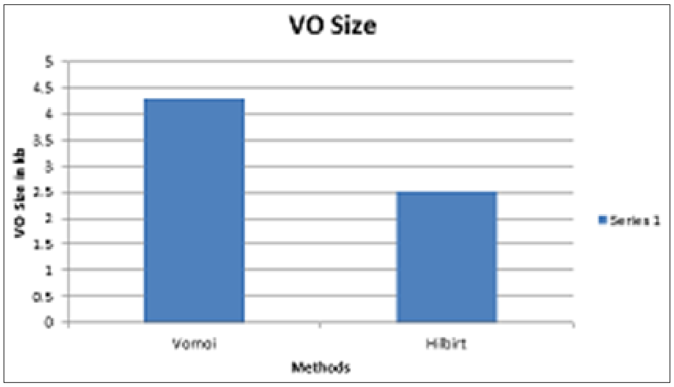

Fig 2

8. Conclusion and Future Work

By using this approach the privacy can be preserved in searching NN for point clouds when the query and object both is moving. Propose system consumes less time than existing by using R-KNN verification and updates to indexing is fast with the help of motion adaptive indexing scheme.

We would like to extend our work by using GPU and CUDA so that it will increase the performance of the system along with it provides privacy in searching NN for MQMO. Using GPU and CUDA the system will be not only scalable but also fast.

9. Acknowledgment

I hereby take this opportunity to express my heartfelt gratitude towards the people whose help is very useful to complete this work “An Efficient algorithm for Privacy in Nearest Neighborhood Search in MQMO for point clouds”. Inspiration and Guidance are invaluable in all aspects of life especially on the fields of gratitude and obligation and sympathetic attitude which I received from my respected dissertation guide, Prof. Prabhudev. S whose guidance and encouragement contributed greatly to the completion of this work.

I express my gratitude to HOD Prof. Joshi S.G for her constant encouragement, co-operation and support. I would like to thank to all faculty members Mrs. Rokade M.R, Mr. Natikar S.B of Computer Engineering Department and all my friends and well-wishers for their co-operation and supports in making this work successful.

I would also like to thank our principal Dr. A.K. Kureshi for his warm support and providing all necessary facilities to me.

Under these responsible and talented personalities, I have been efficiently able to complete my work in time with success.

10. References

1. Charles Asanya, Ratan Guha. Space Partitioning for Privacy in Location-Based Services Continuous Nearest Neighbor Query IEEE Transaction on Mobile computing,
2. Asanya C, Guha R. Anonymous retrieval of k-nn poi in location based services (lbs), in In Proc. WORLDCOMP International Conference on Security and Management, SAM ’13, Jul.22-25, 2013, pp. 294-300.I.S. Jacobs and C.P. Bean, Fine particles, thin films and exchange anisotropy, in Magnetism, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963; 3:271-350.
3. Huang Y, Vishwanathan R. Privacy preserving group nearest neighbour queries in location based services using cryptographic techniques.
4. Xiaolan Y, Zhiming D, Jing J. Moving continuous k nearest neighbor queries in spatial network databases, in IEEE Computer Science and Information Engineering, 2009 WRI World Congress on. 2009; 4:535-541.
5. Ghinita G, *et al.*, Privacy queries in location based services: Anonymizers are not necessary. 2008; 121(132):9-12.
6. Vishwanathan R. Exploring privacy in location-based services using cryptographic protocols, Ph.D. dissertation, Univ. of North Texas, 2011.
7. Shrilaxmi V, Dhamodharan P. Higher Confidentiality through Grouping Hilbert & Voronoi over Validation of K-nearest neighbour query on spatial network.
8. Zheng B, Lee WC, Lee DL. On searching continuous k nearest neighbors in wireless data broadcast systems, in Ieee Transactions on Mobile Computing, 2007, 6.
9. Elmongui HG, Mokbel MF, Aref WG. Continuous aggregate nearest neighbor queries, in Journal on Advances of Computer Science for Geographic Information Systems. 2013; 17:63-95.
10. Tao Y, Apadias D, Shen Q. Continous NN Serach Continous Reverse K-NN queries in Euclidean Space & in spatial Networks, Wenjie Zhang, Xuemin Lin, Ying Zhang.
11. Yao A. How to generate & exchange secres in Proc. of 27th IEEE symposium on foundation of computer science FOCS.

12. Shin H, Atluri V, Vaidya J. A profile anonymization model for privacy in a personalized LBS environment.
13. Vishwanathan R. Exploring privacy in location basee services using cryptographic protocols.
14. Niu B, Zhang Z, Li X, Li H. Privacy-area aware dummy generation algorithm for location based services.
15. Cheema MA, Lin X, Wang W, Zhang W, Pei J. Probabilistic reverse nearest neighbor queries on uncertain data. IEEE Trans. Knowl. Data Eng. 2010; 22(4):550-564, 2010.
16. Cheema MA, Lin W Zhang, Zhang Y. Influence zone: Efficiently processing reverse k nearest neighbors queries. In *ICDE*, 2011, 577-588.
17. www.census.gov/geo/maps-data/data/tiger line.html.
18. www.cs.fsu.edu/%7Elifeifei/SpatialDataset.htm.
19. Yiu ML, Mamoulis N. Reverse nearest neighbors search in adhocsubspaces. IEEE Trans. Knowl. Data Eng. 2007; 19(3):412-426.