SURVEY PAPER ON PRIVACY IN LOCATION BASED SEARCH QUERIES.

Phaltane Anjali .D
Department of Computer Engineering, PUNE University /
Vishwabharati Academy's College Of Engineering, Ahmednagar, India .

Pathan Farheen..F,
PUNE University / Vishwabharati Academy's College Of Engineering, Ahmednagar, India .

Prof.Prabhudev. I,
University / Vishwabharati Academy's College Of Engineering, Ahmednagar, India

ABSTRACT

Due to tremendous growth in mobile phones, the market for Location Based Services is growing fast. Many mobile phone applications uses location based services such as nearest store finder, car navigation system etc. Location – Based Services provides services to mobile device users based on the location information as well as data profile of the users. Using these services mobile users retrieve information about nearest POI. This involves location and data profile of the user's to be misused. In order to protect user's private information many solutions are offered but most of them only addressed on snapshot and no support for continuous query and MQMO .Some papers addressed MQMO but fails to provide privacy. This paper focuses on MQMO and also protect user's private information using PIR (private information retrieval) .

INTRODUCTION

LOCATION BASED SERVICES

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 :

1) Location perturbation
2) Spatial cloaking
3) Temporal cloaking
4) Spatial-temporal cloaking
5) k - anonymity

For Location privacy also different architectures [4] are used such as

1) Client server architecture
2) Trusted third party architecture
3) Peer to peer cooperative architecture

In order to provide 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 moring [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 addrenen snapshot query .

In this paper we proposed 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 & vo size than existing work.

PRELIMINARIES

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.

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

PROBLEM DEFINITION

The administration of transshipment systems 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 vigorously changing and problematical travel conditions. There may be possibilities of user's privacy violated when they are querying about the location information on the third party servers where the location information about the users will be tracked. The malicious attackers may steal 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.

LITERATURE SERVEY

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 proposes 2 technique in order to provide privacy in LBS :

a) Two-tier spatial transformation
b) Three-tier spatial transformation
c) Cryptographic Transformation

Two tier spatial transformation provides direct communication between user & LBS server. But due to waiting for K-N user ,delay in query.

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 provide 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]a n 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 uses 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 of user location 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 asnd 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 Verona 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. 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.

CONCLUSION

We successfully reviewed all papers on privacy in LBS and none of the focus on privacy of LBS in CNNQ in moving query and moving object. The user data may get leaked , because of less security in Voronoi diagram and also the K-NN classification algorithm cannot provide the accurate nearest location information to the user. To overcome these drawback and provide privacy in MQMO of CNNQ we would like to extend our work by using R-KNN with hilbert transform and provide privacy in moving query and moving object using the motion adaptive Indexing.

REFERENCES

[1] Space Partitioning for Privacy in Location-Based Services Continuous Nearest Neighbor Query-Charles Asanya and Ratan Guha

[2]C.Asanya & R.Guha "Anonymous Retrieval of K-NN POI in location based services.".

[3]Y.Huang & R.Vishwanathan,"Privacy preserving group nearest neighbour queries in location based services using cryptographic techniques."

[4]Xan Dzhiming & J.Jind"Moving Continous K-nearest neighbour queries in spatial network databases.

[5]G.Ghinita et al,"Privacy queries in loaction based services :Anonymizers are not necessary."

[6] R.Vishwanatahn ,"Exploring privacy in location-based services using cryptographic protocols ."

[7] V.Shrilaxmi, P Dhamodharan,"Higher Confidentiality through Grouping Hilbert & Voronoi over Validation of K-nearest neighbour query on spatial network.

[8] B.Zheng, W-C Lee & D.L Lee,"On Searching continous K-NN in wireless data broadcast systems."

[9] H.G Elmongui,M.F.Mokbel & W.G.Aref,"Continous aggregate nearest neighbour queries."

[10]Y.Tao,D.Apadias & Q.Shen,"Continous NN Serach"

[11] "Continous Reverse K-NN queries in Euclidean Space & in spatial Networks", Wenjie Zhang,Xuemin Lin, Ying Zhang.

[12] A .Yao,"How to generate & exchange secres"in Proc of 27th IEEE symposium on foundation of computer science FOCS.

[13] H.Shin, V.Atluri & J.Vaidya ,"A profile anonymization model for privacy in a personalized LBS environment."

[14]R.Vishwanathan ,"Exploring privacy in location basee services using cryptographic protocols."

[15]B.Niu, Z.Zhang,X.Li& H.Li,"Privacy-area aware dummy generation algorithm for location based services.".