IPHV2I20006X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

LOCATION BASED SERVICES FOR MOBILE USERS BY QUERY PROCESSING

[1]P.Vasavi , [2]N.Haribabu

1. [M.Tech (CS)] , Dept. of Computer Science & Engineering, JITS, Karimnagar.
2. Professor,Head , Dept. of Computer Science & Engineering, JITS, Karimnagar.

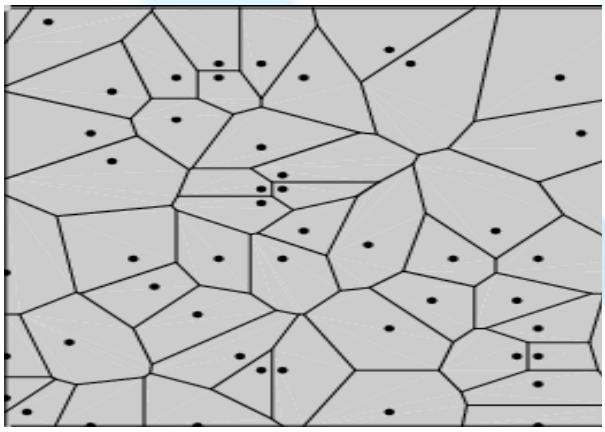
ABSTRACT

The trends of mobile users are drastically changed in their requirement and usage. The common service most of the mobile users are location- based services (lbs). In this application /service ' location plays a key role to provide the service from one side, considerable issue is details of the users are protected. Lbs is to achieve an accurate service, hence it is important to use the mobile user accurate location. Lbs is achieve privacy protection through anonymizer uses k-anonymity cloaking the user location to k- anonymizing spatial region . Our aim is to provide the user privacy through the supposed model.

Key words: *location based service, anonymizer, privacy protection, encryption*

Introduction

A sample Voronoi diagram



Delaunay triangulation

Obtained by connecting the sites in the Voronoi diagram whose polygons share a common edge. It can be used to find the two closest points by considering the shortest edge in the triangulation. Thousands of sensors over strategic locations are used in a structure such as an automobile or an airplane, so that conditions can be constantly monitored both from the inside and the outside and a real-time warning can be issued whenever a major problem is forthcoming in the monitored entity

These wired sensors are large (and expensive) to cover as much area is desirable. Each of these need a continuous

power supply and communicates their data to the end-user using a wired network. The organization of such a network should be pre-planned to find strategic position to place these nodes and then should be installed appropriately. The failure of a single node might bring down the whole network or leave that region completely un-monitored. Unattendability and some degree of fault tolerance in these networks are desirable in those applications where the sensors may be embedded in the structure or places in an inhospitable terrain and could be inaccessible for any service

Undoubtedly, wireless sensor networks have been conceived with military applications in mind, including battlefield surveillance and tracking of enemy activities. However, civil applications considerably outnumber the military ones and are applicable to many practical situations. Judging by the interest shown by military, academia, and the media, innumerable applications do exist for sensor networks. sensor networks is flourishing at a rapid pace and still there are many challenges such as:

- Energy Conservation - Nodes are battery powered with limited resources while still having to perform basic functions such as sensing, transmission and routing
- Sensing - Many new sensor transducers are being developed to convert physical quantity to equivalent electrical signal and many new development is anticipated
- Communication - Sensor networks are very bandwidth-limited and how to optimize the use of the scarce resources and how can sensor nodes minimize the amount of communication
- Computation - Here, there are many open issues in what regards signal processing algorithms and network protocols

Encryption:

This algorithm takes a message *M*, the public key *PK*, and a set of attributes *I* as input. It outputs the cipher text *E* with the following format:

***E* = (*I*, ˜ *E*, {*Ei*}*i*)**where ˜*E* = *MY*, *Ei* = *Ti*.

Secret key generation:

This algorithm takes as input an access tree *T*, the master key *MK*, and the public key *PK*. It outputs a user secret key *SK* as follows.

***SK* = {*ski*}**

Decryption:

This algorithm takes as input the cipher text ***E*** encrypted under the attribute set **U**, the user's secret key ***SK*** for access tree ***T***, and the public key ***PK***.
Finally it output the message ***M*** if and only if **U satisfies T**.

2) Proxy Re-Encryption (PRE):

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext. A PRE scheme allows the proxy, given the proxy re-encryption key ***rka↔b,*** to translate cipher texts under public key ***pk1*** into cipher texts under public key ***pk2*** and vise versa.

3) Lazy re-encryption:

The lazy re-encryption technique and allow Cloud Servers to aggregate computation tasks of multiple operations. The operations such as
Update secret keys
Update user attributes.

Existing Model

- Existing techniques cannot be used effectively in a wireless broadcast environment, where only sequential data access is supported.
- It may not scale to very large user populations.
- In an existing system to communicate with the server, a client must most likely use a fee-based cellular-type network to achieve a reasonable operating range.
- Third, users must reveal their current location and send it to the server, which may be undesirable for privacy reasons

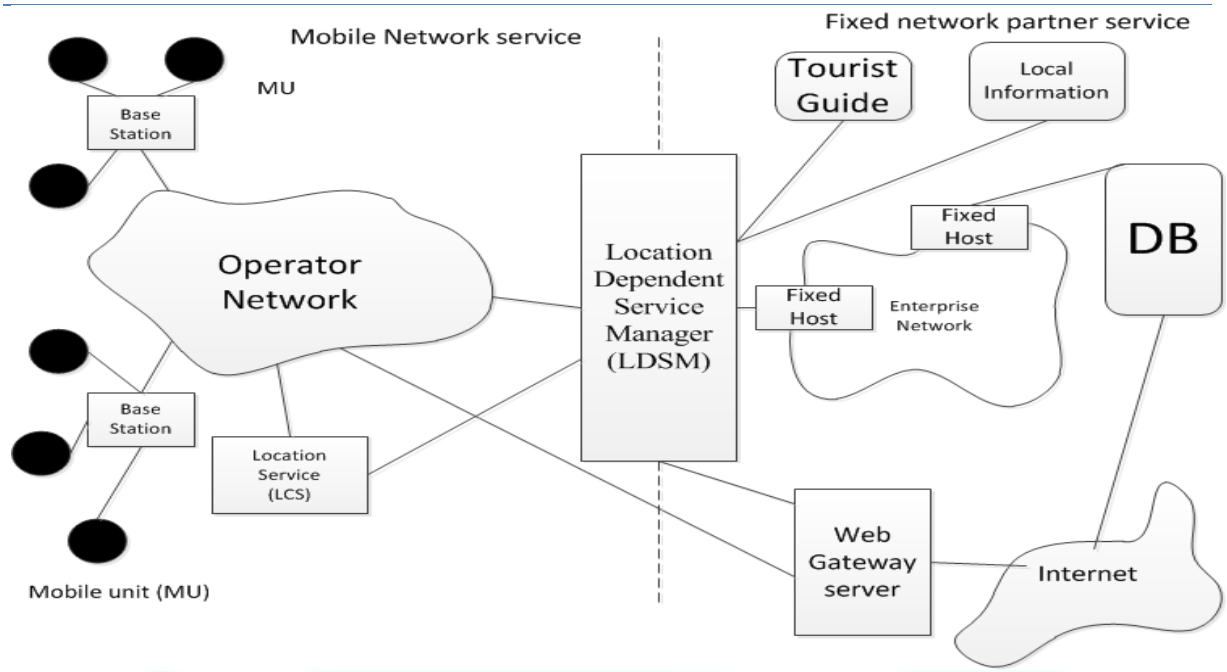
Proposed Approach

This System is a novel approach for reducing the spatial query access latency by leveraging results from nearby peers in wireless broadcast environments.

Our scheme allows a mobile client to locally verify whether candidate objects received from peers are indeed part of its own spatial query result set.
The method exhibits great scalability: the higher the mobile peer density, the more the queries answered by peers.

The query access latency can be decreased with the increase in clients.

IPHV2I20006X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245



Modules

- Wireless Data Broadcast
- Sharing-Based Nearest Neighbor Queries

Wireless Data Broadcast

- In general, there are two approaches for mobile data access.
- One is the on-demand access model, and the other is the wireless broadcast model.

For the on-demand access model, point-to-point connections are established between the server and the mobile clients, and the server processes queries that the clients submit on demand. For the wireless broadcast model, the server repeatedly broadcasts all the information in wireless channels, and the clients are responsible for filtering the information.

An example of such a system is the Microsoft Direct Band Network.

The advantage of the broadcast model over the on-demandmodel is that it is a scalable approach.

- However, the broadcast model has large latency, as clients have to wait for the information that they need in a broadcasting cycle.If a client misses the packets that it needs, it has to wait for the next broadcast cycle.

IPHV2I20006X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .2
ISSN Online: 2319 – 9253
Print: 2319 – 9245

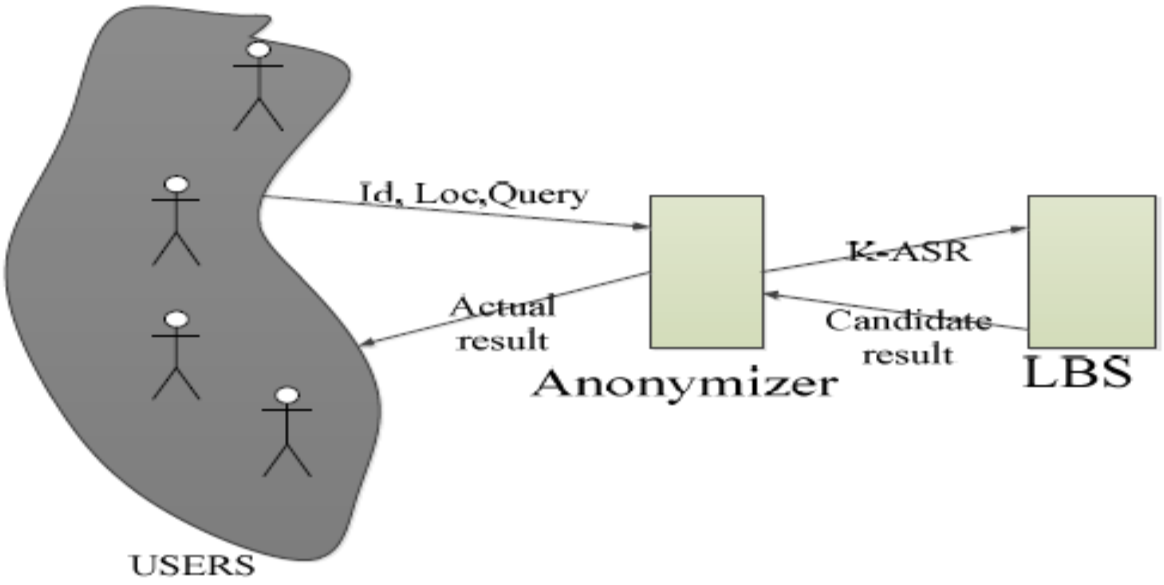


Fig-2: Architecture of traditional K- Anonymity

Sharing-Based Nearest Neighbor Queries

- At first, by scanning the on-air index, the k-nearest object to the query point is found, and a minimal circle centered at q and containing all those k objects is constructed.
- The MBR of that circle, enclosing at least k objects, serves as the search range. Consequently, q has to receive the data packets that covers the MBR from the broadcast channel for retrieving its k-nearest objects.
- The other problem with this search algorithm is that the indexing information has to be replicated in the broadcast cycle to enable twice scanning.
- The first scan is for deciding the kNN search range, and the second scan is for retrieving k objects based on the search range.
- Therefore, we propose the Sharing-Based Nearest Neighbor(SBNN) query approach to improve the preceding on-air kNN query algorithm.
- The SBNN algorithm attempts to verify the validity of k objects by processing results obtained from several peers. Table 1 summarizes the symbolic notations used throughout this section.

Conclusion

Finally we conclude that the supposed framework to provide the protection to location-based services for the mobile

users. it gives better security& strong defense system from the attack of the attacker. The main goal of this article is to the framework gives accurate result quickly and does not store user profile info due to the reasons of hacking. The proposed system has better performance than compared to the earlier existing system with SBNN and KNN.

REFERENCE

[1] Srikanth, Awasthi, "Voronoi-based Continuous query processing for mobile users", IEEE International Conference on Communication Systems and Network Technologies, 2011.

[2] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in

[3] Anonymous Spatial Queries." In *IEEE TKDE*, 2007.

[4] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Priv´e: Anonymous location-based queries in distributed mobile

[5] systems," In *WWW*, 2007.

[6] 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.

[7] M. L. Yiu, C. Jensen, X. Huang, and H. Lu, "Spacetwist: Managing the trade-offs among location

[8] privacy, query performance, and query accuracy in mobile services," In *ICDE*, 2008.

[9] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Int. Workshop on Multimedia and Security*, 2001, pp. 27–30.

[10] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[11] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.

[12] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," *Signal Process.*, vol. 90, no. 11, pp. 2954–2964, 2010.

[13] [14] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme," *IEEE Signal Process. Lett.*, vol. 14, no. 11, pp. 848–851, Nov. 2007.