Persistency Based Ad-hoc Broadcast Protocol for Location Privacy in LBS applications

Balaso Jagdale
G H Raisoni College of Engineering, Nagpur, RTMN University,
Digdoh Hills, Hingana Road, India
bjagdale@gmail.com

Jagdish Bakal
S S Jondhale College of Engineering, Thane, Mumbai University,
Manpada Road, Dombivali, India
bakaljw@gmail.com

Abstract **– It is vital to manage mobile users' privacy and quality of service in location aided services and applications. Today's architectures and model are all commercial oriented, which underweights the privacy and highlights the quality of services. It results in loss and misuse of privacy. Different authors have proposed architectures and methods to protect location privacy. These architectures are three tier, multi-tier, centralised, distributed. We have proposed peer to peer, cooperative broadcast users model to protect mobile users privacy. Our motivation lies in the natural human process of enquiry. When user reaches to unfamiliar area, user enquires the local user about point of interests. Local user is persistent in that area and has lot of knowledge of that area. Mobile user just asks query to local user and does reveal about his identity. So all users are persistent and expert in their local areas or areas where they spend more and more time.**

Technically, every user stores in its mobile device points of interests. This database is his knowledge of POIs in his persistent area. Requester user broadcasts his query, and other local user also broadcasts POI replies, if answer is in his database. In summary, this is a peer to peer, broadcast, client server, and distributed request-reply model. Next, POIs learning is done from government authorised, centralised trusted server, by the mobile users. So every mobile device has to study its own persistency and based on that information, download and maintain POIs in its data base system. So that user can cooperatively share whatever POI knowledge he has. We have designed such a system, implemented and analysed such system. We have also analysed the privacy, performance, persistency optimization in this work. We found that this mechanism is stronger to protect the location privacy but it is a challenge to address cooperative nature of human being and commercial aspect of service providers.

Keywords— Cooperative networks, Persistency, Location Privacy, Spatial Cloaking, Location Based Services.

I. INTRODUCTION

Recent technologies allow to measure and track location of object. Few of the technologies such as GPS gives location in the form of Longitude and Latitude. Positioning systems collect huge amount of this sensitive location information. Actions of user are usually associated to the location e.g. searching the nearest gas station, nearest Hospital etc. The various location based services are classified into various categories according to your functionality viz., navigation, tracking information, billing and social networking. Subsequently, several profitable and enterprise-oriented LBSs are operating and achieving progress. A key aspect for development of LBS services is reduced cost of mobile devices and integration of location based technology in existing telecommunication infrastructure is economically feasible.

Location Based Services:

Number of location aided services are offered these days such as taxi hiring system, friend finder, nearby shop finder etc. Mostly architectures are centralised where user shared his or her location and get the service. Now a days intelligent LBS applications are also being launched which involves business and individual analytics based on location information. IT laws fails to be time ready to protect the location privacy. There are legal, social, commercial, political and technical aspects for the privacy. We are concerned about attacks on location information and its protection from malicious hands.

Location Privacy:

Formally, Location Privacy is demarcated as the guarantee of mobile users to agree as when, and for which determinations their position information could be used by relevant businesses. Revealing location knowledge, could make attacks possibility by rivals. There could be following categories of privacy:

1. Identity Privacy: It is to protect user's identities related to location.
2. Position Privacy: It is to protect user's actual location or position.
3. Path Privacy: To protect the path that user is continuously monitoring for certain period of time.

Motivation:

There are generally three dissimilar mechanisms for achieving the privacy in LBSs. In the non-cooperative approach, the users use their own ability to hide their location using hiding techniques such as pseudonymity and dummies. The centralized trusted third party (TTP) method banks on a rusted third party that cloaks the location of the mobile user who requests for the services with the anonymised location and returns the result to the users. Yet in peer-to-peer cooperative approach, a group of users cooperatively hide their location information. In this case, the union of the users leads to their anonymization. The first mechanism is simple in strategy but susceptible to numerous attacks. The second approach suffers from TTP being a bottleneck, although it is the most accurate approach and provides the maximum privacy level. In the last approach, users collaborate to cloak their locality information in a scattered way in order to attain privacy leading to Privacy-Quality of Service (QoS) trade-off.

Based on various categories of Location Privacy, there are different techniques are introduced as follows.

Anonymity Based Technique:

This provides solution for the identity based and path based location privacy. This technique allows individual to be unidentified.

K-anonymity based approach means user is clubbed with additional K-1 users. This way user is cloaked in crowd and indirectly protected privacy. More the K factor, more the crowd, more the protection. So privacy is proportional to K factor.

Obfuscation Based Technique:

These technique involves changing addresses, varying distances, manipulation of longitude and latitudes, cloaking area sizing. Application specific protection solutions are normally designed with these techniques.

Policy Based Technique:

Management of location is the important issue as it satisfies the objectives of multiple entities involved in LBS applications. We can have hierarchical, organised, policy based approach that implements access control with cryptography and software controls.

Amongst above three techniques k-anonymity technique can be seen as a state of being unable to identifiable among several objects. K-anonymization refers to hiding one's identity among k-1 several users in the same cloaking region. Here Trusted Third party does the anonymization of location of requesting user and sends back the pseudonym. Assumed that, TTP possess location of other users within the same region.

II. LITERATURE SURVEY

Xiao Pan et al. [1], demonstrated attacks on location updates of mobile users due to continuous movements. They designed incremental cloaking of groups for protection. Formally implemented with graphs to maintain the maximum groups that takes care of continuous movement. To contain various location privacy threats many techniques have been developed for safeguarding location privacy such as k-anonymity principles, generation of dummies, encryption etc. Ali and others, [2] have shown the taxonomy of privacy mechanisms, which are mostly based on cloaking tricks. Eran Toch [3] has studied empirically privacy implications based on wider mobility of users. Authors in [4, 5 and 6] discuss about location privacy threats, k-anonymity based solutions and inference attacks. Mohamed F. Mokbel [7, 8], privacy protection idea is based on a third trusted party, where in Anonymizer Server, gets the exact location of requester. AS then purterbates user with cloaking method in spatial form and send this cloaking region to LBS server. Set of POIs answered to AS server. And finally filtering is done for exact POIs nearest to mobile user. Still Privacy strength and Quality of Service is not clearly presented in the said work. Chi-Yin Chow et al. [9], proposed a peer to peer technique that is close to our proposed work, where users for peer groups. Some static members will help find POI answers. They have also considered cloaking in the region. They have studied performance, communication cost and quality of service. Our work is different from that of Chi-Yin, as we have proposed only one hop client server, no cloaking computation, and local database management among peers based on persistency or mobility history. Our results cannot be directly compared with above authors because of architecture differences. Maria and other in [11] have done survey in 2014 and gave the status of current research in location privacy. They have also proposed conceptual models. Gang and Victor have proposed algorithm for protection of privacy and studied performance of LBS replies [12]. Peer to Peer model are not exhaustively studied by earlier authors.

Drawbacks of Existing Approaches:

1. Non-cooperative Approach-simple in design but vulnerable to several attacks.
2. Centralized Approach-trusted third party is the bottleneck, privacy/quality trade-off.
3. Peer-to-peer Approach-assuming all users are trusted, costly communication, privacy/quality trade-off.
4. Real Life Example of Knowledge Sharing

III. PROPOSED RESEARCH WORK

Proposed work is to design a protocol, local database system, peer-to-peer request reply model, for enabling location privacy in location based applications, by reducing the computations & performance overheads, and providing better Quality of Services. More over effectiveness of such an architecture is analysed.

Features

- Broadcast based Knowledge Sharing:

The persistent user of a particular region will have nearby POIs in their local database. Hence, whenever a user enters a new region he/she can broadcast a request for nearby POIs to the users who are persistent in the region & will get the reply.

- Persistent POI Database

The user will only store the POIs for the region where he/she is more persistency. Hence, removing the overhead of storing unnecessary POIs. The POIs are dynamically added to the database based on the user's persistency in the region. If the user's persistency in a region decreases over the period of time, then the corresponding POIs for the region are also deleted accordingly.

- Safe Governance

As the mobile clients are requesting POIs for regions, their exact location will not be revealed to LBSD Server. Moreover we are utilizing broadcast based request reply model for POI exchange, hence keeping the identity of the users hidden from each other.

- Authenticated POIs

The Government POI authentication Server will make sure that all the POIs are correct. This will avoid use of POIs with wrong information.

Objectives

To study the performance overhead for anonymous broadcast protocol for knowledge sharing.

To design and implement persistency to optimize the local POI database in mobile users devices. Server based signed document system for the clients & servers.

To study the requirement of sampling frequency for computation of persistency.

Scope: Range limit for Bluetooth & Wi-Fi
Bluetooth Usage
Among different Bluetooth parameters, there are two most widespread classes (categories) of devices:
Class 1: distance up to 100 meters (in most types 20-30 meters)
Class 2: distance up to 30 meters (in most types 5-10 meters)
Wi-Fi Usage
A general wireless access point uses 802.11b or 802.11g including a stock antenna may have a distance of 32 mtrs. (120 ft.) Inside and 95 mtrs. (300 ft.) Outside.

This broadcast based request reply is a cooperative architecture where by Users are not bounded to participate in the system. In this cooperative architecture, users are not bounded to participate in the system.

Research Methodology: We are proposing a novel architecture for enabling location privacy in Location based Application using Broadcast Based Message Exchange Protocol. As the computation power of mobile devices have increased over the years, it is now possible to perform resource hungry computation on them. In this system a mobile user will keep logging GPS Traces at a certain frequency. Based on these GPS traces, circular regions are formed having radius 200 meters. The regions are created dynamically for each mobile. As soon as a GPS location is received, corresponding region is searched for in the database. If a region is found to which this location belongs the time spent parameter for the region is updated. If no region is found for the location, then a new region is created with location as the centre. Because of this there can be overlapping regions also in the system. If a location is found in more than one location then the region whose centre is close to the location is considered to the appropriate region for the location.

We have assumed our parameters for the computation of persistency of a user for a region. The four parameters are:

1. Time Spent in the Region (Thrs)
2. Number of Requests for POIs of a Region (ReqCtr)
3. Number of POI Replies for a Region (ReplyCtr)

We have assigned some weights to each of these four parameters, based on our assumption for their dependency for persistency calculation.

As time spent in a region will be a major factor for user's persistency in a region, that's why it have been given 80% weightage. The next two parameters, no. of requests & no. of replies, will also play a significant role in user's persistency in the region, so each of them has been assigned with weightage 10% each.

Since we are computing the persistency value for a region on a daily basis, we have assumed the upper limits for parameters, Time spent outside, Requests Counter & Reply Counter to be 8 hours, 5 Max, 5 Max respectively. So the formula for persistency calculation for a day will be:

Persistency Value P for a Region is,

$$P = \left(\frac{THrs}{8} \times 80 + \frac{ReqCtr}{5} \times 10 + \frac{ReplyCtr}{5} \times 10 \right) /100$$

Any changes to any of the four parameters will result in calculation of persistency value for the region. For example, if a request for POIs of a region is received, the request counter for that region will be incremented & persistency value will be calculated for the region. Same will be the case for replies, personal queries & time spent in the region. The reason behind this method is, want to fetch the list of POIs from the LBSD Server as soon as the minimum threshold persistency value for a region has been reached. Initially we have assumed the minimum threshold persistency value to be 0 hours, 0 Request Counter, 0 Reply Counter.

The Location based Database Server is used to get POI list with respect to the latitude & longitude provided. The LBS Server uses spherical rule of cosines formula in order to compute distance between two Geo locations.

The formula to compute the distance amid two geo locations using the spherical rule of cosines is:

$$Distance = Cos\big(Sin(Lat1) \times Sin(Lat2) + Cos(Lat1) \times Cos(Lat2) \times Cos(Long2 - Long1)\big) \times R \; Where \; R \; is \; Earth \; Radius \; 6371KM$$

The response from the server is in the JSON format.

The user's persistency for each region is averaged daily and is compared with the minimum threshold persistency value. If the average persistency value for a region is less than the minimum threshold value, the corresponding percentages of Point of Interests are deleted for the region from the database. This helps in maintenance of user mobile's local database. This means if the user is not persistent in any region anymore, then the corresponding POIs for that region are automatically removed from the database. The POIs are deleted on the basis of their distance from the center of the region, i.e. the POIs that are far away from the center are deleted first.

The Broadcast based Request Reply Message Exchange protocol helps the users to exchange the persistent POIs with each other. Knowledge Sharing is the main idea behind this message exchange protocol. The user who is having more persistency in a particular region will have the POIs of the same region. Whenever a new user arrives in that region, he/she can broadcast's his/her request for certain POIs to these persistent users and get the required POIs from them. This protocol maintains the anonymity of the users in the system. If the persistency of the user decreases for a particular region the POIs for that region are deleted accordingly, i.e. in decreasing order of their distances from the center of the POI. Due to this, the overhead of storing large number of POIs is reduced.

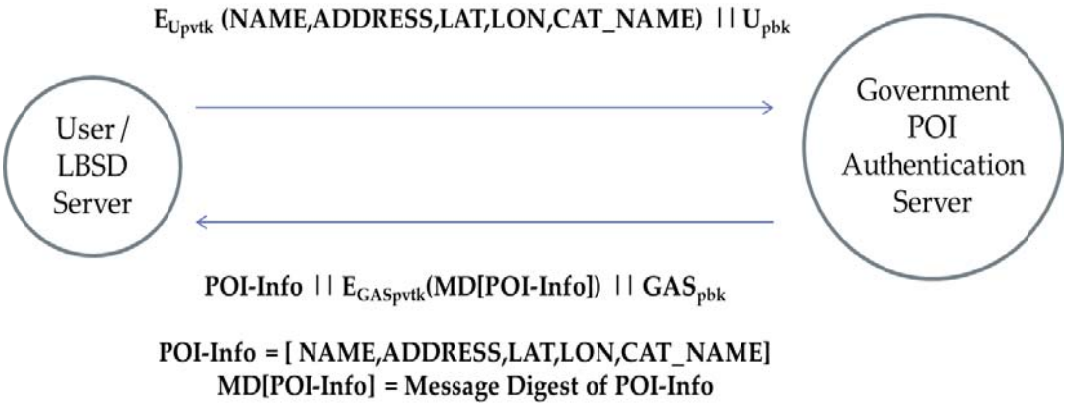


Figure 1. POI Authentication System

We are also proposing a POI Authentication System, as shown in figure 1. The user or the LBSD Server can register new POI at the Government POI Authentication Server (GAS). We are using public key cryptography for encrypting the messages. The request is encrypted using sender's private key & then this encrypted request is sent to the server along with the sender's public key. The administrator at the GAS will decrypt the request & will verify the POI information. On successful verification the admin will sign the POI with its private key. This signature will be appended along with the POI information and sent back to the requestor, which maybe a user or LBSD Server

System Architecture

As shown in figure 2, A Mobile node can broadcast request query for any point of interest i.e. POI through WLAN, that request is received by all nodes that are within its Wi-Fi range. Every Mobile node has its own local database of POIs. The receiver node processes the request query with respect to their local POI database and respond accordingly.

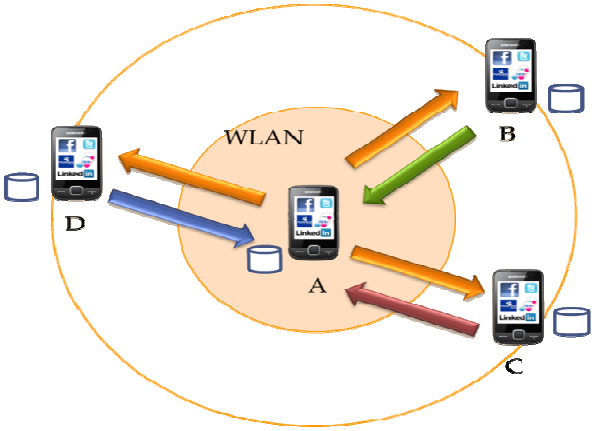


Figure 2. System Architecture-Part 1

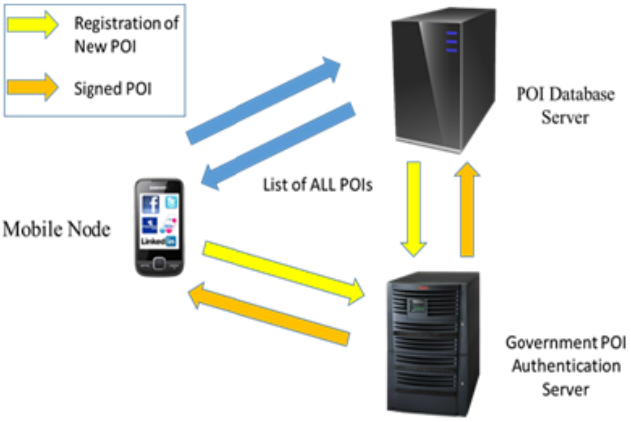


Figure 3. System Architecture-Part 2

Whenever any new Mobile node enters into the system (Figure 3), it requests the Centralized POI database server for the list of all the POI of that particular region, then POI Database Server process request & sends the list. On arrival of the POIs list, the requesting mobile node will filter list of all POIs as per its current location & store them in its local database.

In this architecture, there is a Centralized Government Authentication Server which provides the POIs authentication service using public-key cryptography (e.g. RSA or Diffie-Hellman). Whenever a Mobile Node or POI Database Server, wants to add a new POI to their database; they first have to register their new POI with the Government Authentication Server. The Government Authentication Server verifies the new POI that has been sent for the registration & after successful verification it then encrypts the POI with its private key and send the cipher text data along with the public-key to the requestor. On receipt the requestor will decrypt the signed-POI with the public-key & will store the POI into its database. It is the task of the requestor in the broadcast-reply scenario to authenticate the received POI with Government POI Server.

This system strives for maintaining persistent local database for each Mobile Node. Each Mobile Node maintains a COUNTER value for each POI in the database. It increments the COUNTER value of the POI, whenever it is nearby it & vice versa. If the COUNTER value decreases below the threshold value, then the POI is deleted. In this way, persistent POIs are maintained in the database.

Database Design Model: In this section database model is presented which is required to be established. We have mobile user database design, POI server or LBS server and third is government controlled server

User Device Database

POI_TABLE	
POI-ID	INTEGER
NAME	VARCHAR(100)
ADDRESS	VARCHAR(100)
LATITUDE	DECIMAL(8,6)
LONGITUDE	DECIMAL(8,6)
CATEGORY	TEXT(40)
EMD	VARCHAR(300)
REGION_ID	INTEGER

REGION_TABLE	
REGION-ID	INTEGER
LATITUDE	DOUBLE
LONGITUDE	DOUBLE
TIME_SPENT	DOUBLE
REQUEST_COUNTER	INTEGER
REPLY_COUNTER	INTEGER
QUERY_COUNTER	INTEGER
CREATION_DATE	DATETIME
LAST_UPDATE	DATETIME

PERSISTENCY_VALUE_TABLE	
REGION_ID	INTEGER
DATE_TIME	DATETIME
PERSISTENCY_VAL	REAL

Figure 4. Mobile DB Model

Centralized POI Server Database

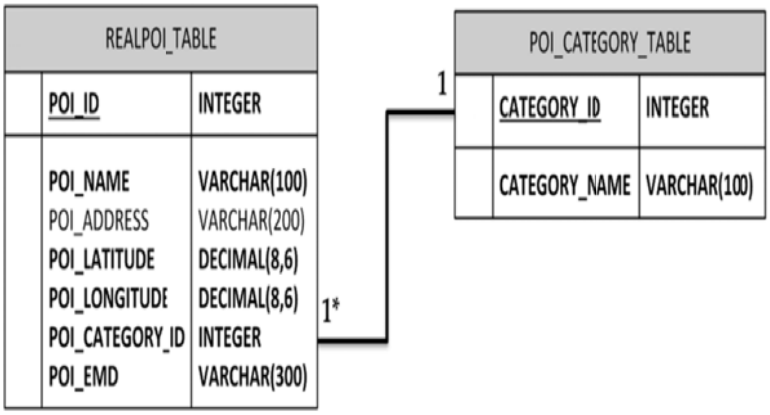


Figure 5. REAL POI DB Model

Government POI Authentication Server

REGISTRATION TABLE
USER-ID
NAME
BUSINESS-TITLE
ADDRESS
MOBILE-NO
EMAIL
STATUS
DATE

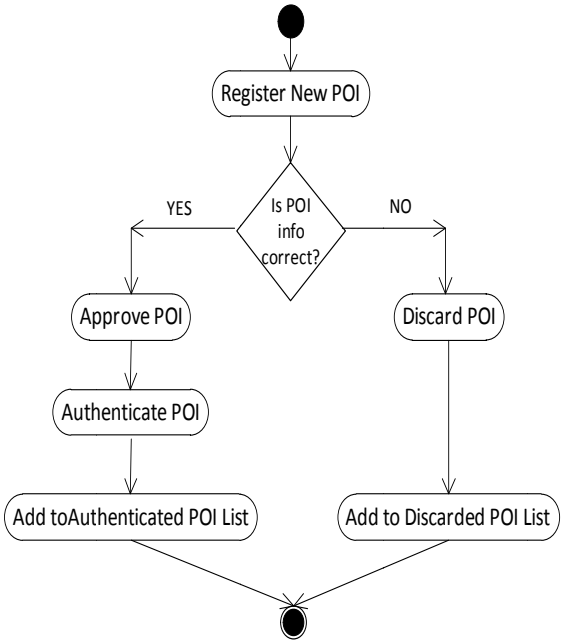
POI TABLE
POI-ID
NAME
ADDRESS
LONGITUDE
LATITUDE
CATEGORY
STATUS
SIGNATURE

Figure 6. Govt. Authentication Server database

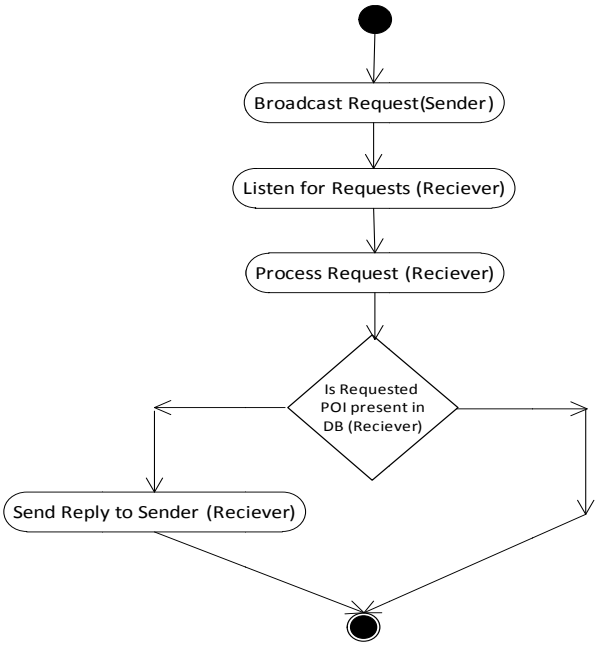
We have carried out a number of experiments on our system & results have been compiled based on them. In this section we'll go through each experiment & analyse the results.

Persistency Computation Steps and Flowcharts

Having been shown the architecture and idea of privacy using peer to peer model and persistency computation, following activity diagrams explains the logic of LBS working, cloaking flow and steps for various activities.



Activity 1: POI Authentication between Mobile User and Govt. Server

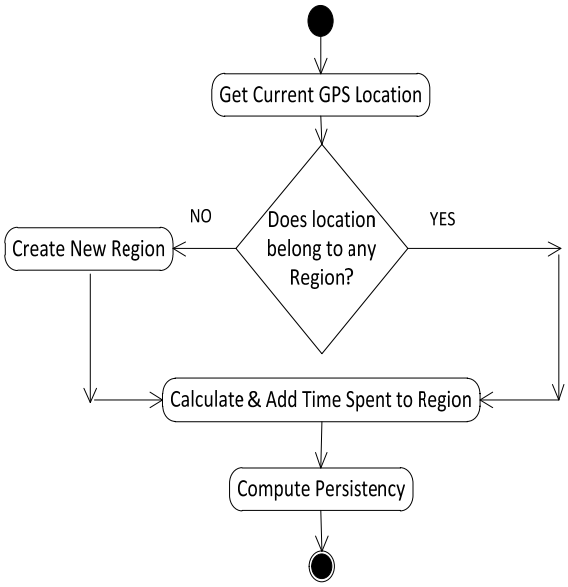


Activity 2: Broadcast based Request Reply Steps

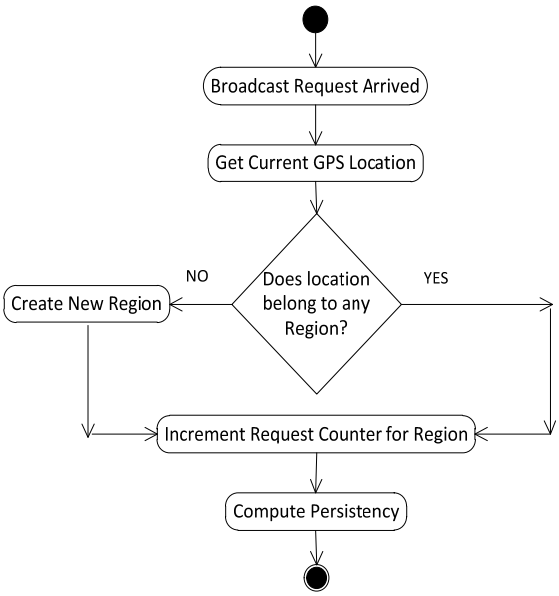
Maintaining persistent POIs based on four parameters, Time Spent, Request counter, Reply Counter & Personal Query Counter are as follows.

IV. RESULTS AND ANALYSIS

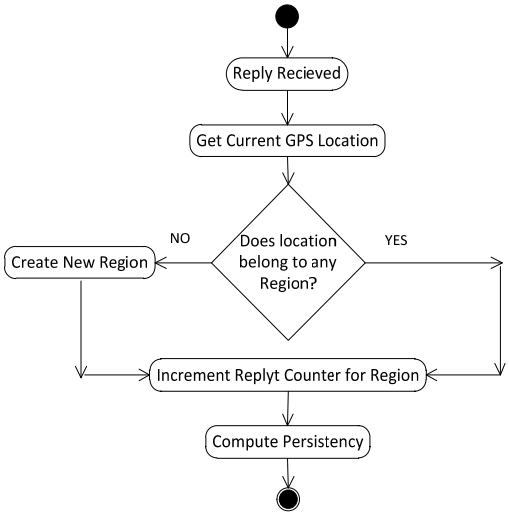
We have created system prototype where Authentication Server, POI DB server is set and mobile application is run in two mobile devices so that one act as requester and other answers query. The experiments and their outcomes are as shown below.



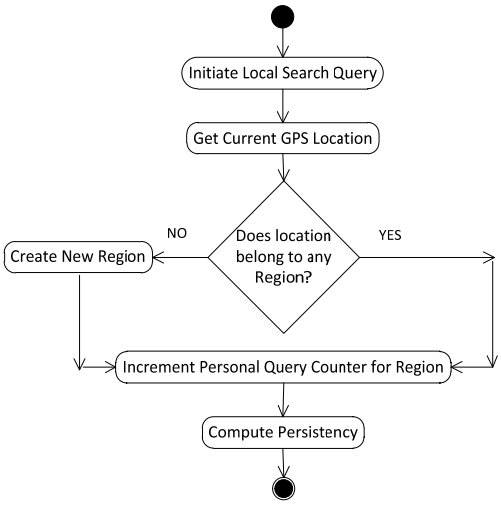
Activity 3: Time Spent: Persistency Calculation for Time Spent in Region



Activity 4: Request Counter: Persistency Calculation for No. of Requests for a Region



Activity 5: Reply Counter Persistency Calculation for No. of Replies for a Region



Activity 6: Personal Query Counter: Persistency Calculation for No. of local queries for a Region

Experiment-1: Evaluate the Performance of Government POI Authentication Server

We have automated the authentication process of GAS Server & have calculated the performance of the system based on 4 parameters; Overall Time Taken (msec.), Average Server's Processing Time (msec.), Average Client's Processing Time (msec.) & Communication Time (msec.).

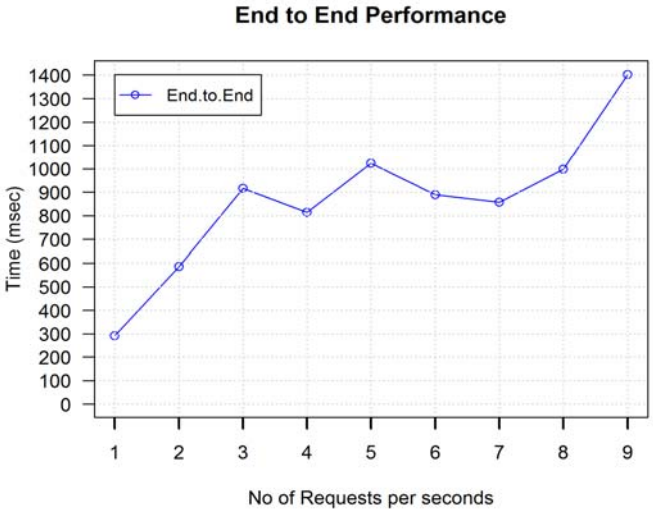


Figure 7. End to End system performance

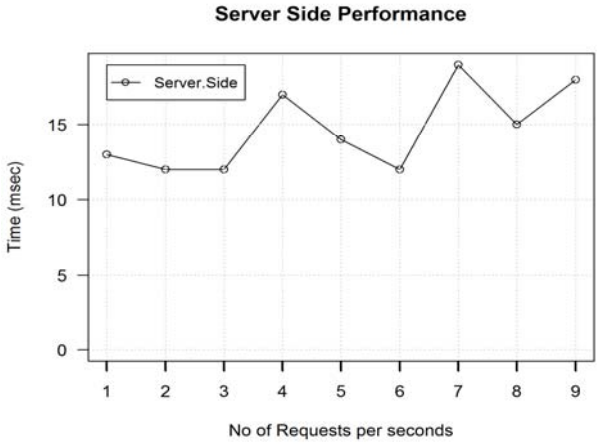


Figure 8. GAS Server Performance

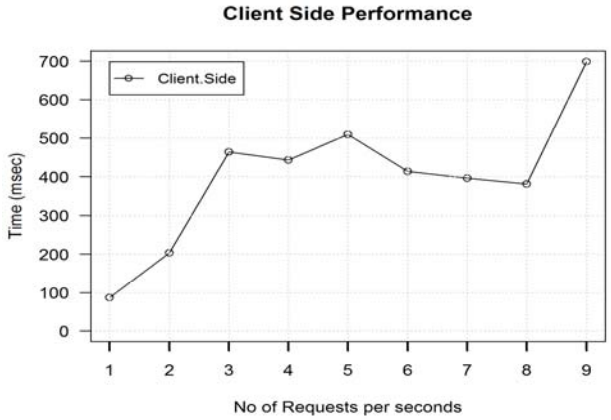


Figure 9. Client device Performance

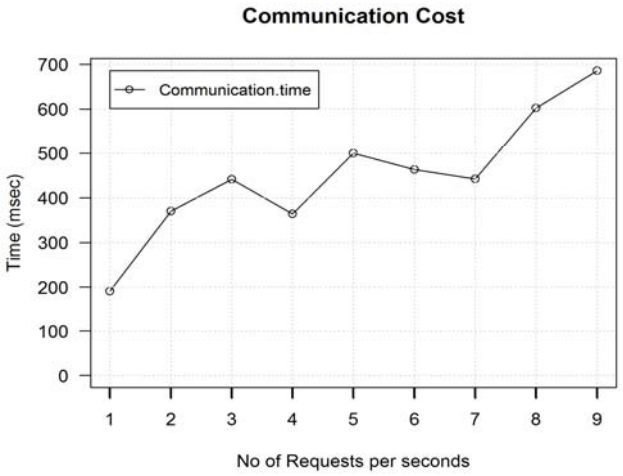


Figure 10. Communication Cost

The Overall Time Taken for Request-Reply is directly dependent on the GAS's Processing Time, Client Mobile's Processing Time & Communication Cost. As we can see in figure 8, the Server's average processing time is near about same for requests up to 9/sec.

Experiment-2: To Study the impact of GPS Traces Frequency on Persistency Computation.
We have set the frequency of GPS Trace initially to 30 secs. & have increased it day by day. Also, we are saving the time taken for Persistency Computation in a log file named "Persistent-Comp.txt". This experiment is carried for only one user. The persistency log is filtered based on the time duration 7am-7pm for the user.

Experiment-3: To study the impact of GPS Traces Frequency on Persistency Value.
We have set the frequency of GPS Trace initially to 30 secs. & have increased it day by day.

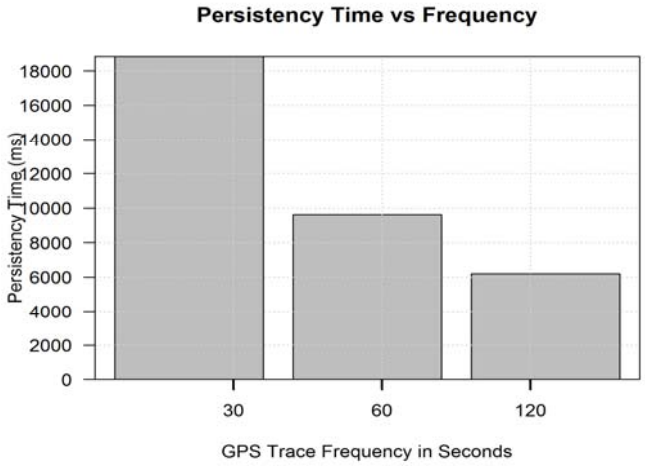


Figure 11. Impact of GPS Trace Frequency on Persistency Computation

As we can see in figure 11, the persistency computation time decreases as the GPS Trace frequency increases. Hence, the battery life of the mobile increases with increasing GPS Trace Frequency. Also, we are saving the persistency value of each region in a log file named "Persistency.txt". This experiment is carried for only one user. The persistency log is generated at the end of each day.

From the figure 12, we can learn that there is no much impact of sampling frequency on persistency value accuracy in this application. But normally more sampling gives better accuracy or quality of any calculations. Since persistency is in hours, few minutes sampling rate is reasonable to settle for persistency.

This also saves lot of device power required for calculation. In our experiment in Pune (India) regions, Region 6 (kothrud) is having higher persistency value for GPS trace frequency 120 sec. as compared to 60 sec. GPS trace frequency. It is natural to have good persistency at least at two places. Residence and office regions of user will have very good persistency. For other regions, persistency may vary as per the time spent by mobile user in the new regions. User stay or persistency is required in POI database building and its maintenance.

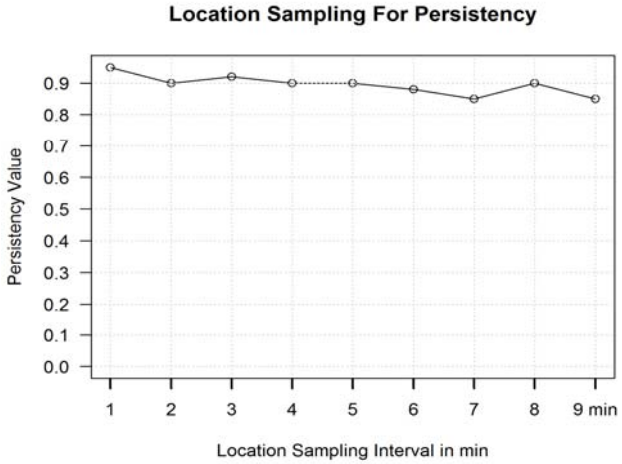


Figure 12. Location sampling impact

V. CONCLUSION AND FUTURE SCOPE

The goal of this research project was to achieve location privacy. This is done by introducing peer to peer broadcast protocol for LBS request – reply model. While on one side we achieve the privacy, as an overhead we need to spend mobile energy in the form of computing and communication cost. Persistency idea of mobile user is introduced to maintain local and neighborhood POI database. Exchange of POI information among themselves cooperatively substantially improves location privacy of mobile users. Experiments shows that persistency value calculation can be accurately done by setting location sampling frequency in terms of few minutes instead of seconds.

Future scope is to create detailed prototype system with real cloud servers, and users in the system. Rewards can be provided for the best service providing cooperating mobile nodes in this system.

ACKNOWLEDGEMENTS

This research project is supported by G. H. Raisoni College of Engineering, Nagpur and MIT College of Engineering, Pune where infrastructure support was available in the research labs. My graduate student, Sujay Meshram, contributed for programming in Android and Java Programming. Moreover, we are thankful to Prof. Vivek Deshpande for valuable inputs regarding architecture.

REFERENCES

[1] Xiao Pan, Jianliang Xu, and Xiaofeng Meng, “Protecting Location Privacy against Location-Dependent Attacks in Mobile Services”, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENG., IEEE TKDE, 2011.
[2] Ali Khoshgozaran and Cyrus Shahabi, “A taxonomy of approaches to preserve location privacy in location-based services”, Int. J. Computational Science and Engineering, Vol. 5, No. 2, 2010.
[3] Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y.Tsai,Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, Norman Sadeh.“Empirical Models of Privacy in Location Sharing”, UBI comp, ACM 978-1-60558-843-8/10/09, ACM, 2010.
[4] Kazuhiro Minami and Nikita Borisov, “Protecting Privacy against Inference Attacks”, CCS, ACM 2010.
[5] Ali Khoshgozaran, Cyrus Shahabi and Houtan Shirani-Mehr, “Location privacy: going beyond K-anonymity, cloaking and anonymizers”, Springer, 2010.
[6] Joseph Meyerowitz and Romit Roy Choudhary. ”Realtime Location Privacy via Mobility Prediction”, ACM 2009.
[7] Mohamed F. Mokbel,Chi-Yin Chow, and Walid G. Aref, “The New Casper: A Privacy-Aware Location-Based Database Server”, IEEE, 2007.
[8] Mohamed F. Mokbel, “Towards Privacy-Aware Location-Based Database Servers”, Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06), 2006.
[9] Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu, “A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services”, ACM-GIS, 2006.
[10] Android Documentation: http://www.developer.android.com/training/index.html
[11] Maria Luisa Damiani, “Location privacy models in mobile applications: conceptual view and research directions”, Geoinformatica, 18:819–842 DOI 10.1007/s10707-014-0205-7, Springer 2014.
[12] Gang Sun and Victor Chang, “L2P2: A location label based approach for privacy preserving in LBS”, http://dx.doi.org /10.1016/j.future.2016.08.023, 0167-739X/© 2016 Elsevier, 2016.

AUTHORS PROFILE

B N Jagdale, BE Computer Engineering degree from Pune University in 1992. He received ME in Computer Engineering, from VJTI, under Mumbai University in 1999. Presently he is pursuing Ph.D. in the field of Information Security from GH Raisoni College of Engineering affiliated to RTM Nagpur University, India. He is presently working as an Associate Professor at the Department of Information Technology at MIT College of Engineering, PUNE, INDIA. He has more than 23 years of academics experience including head of computer department at SPCE, Mumbai His research interests in Information Security and more specific, Information Privacy. He has also a Certified Ethical Hacker certification from EC Council in his credit. He is Professional Member of ACM and life Member of CSI, IETE, ISTE INDIA.

Dr. J. W. Bakal received MTech from (EDT), Electronics Design and Technology Department, from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Later, He completed his Ph.D. in the field of Computer Engineering from Bharati Vidyapeeth Deemed University, Pune. He is presently working as Principal at the S.S. Jondhale College of Engineering, Thane, India. In Mumbai University, he was on honorary assignment as a chairman, board of studies in Information Technology and Computer Engineering. He is also associated as chairman or member with Govt. committees, University faculty interview committees, for interviews, LIC or various approval work of institutes. He has more than 27 years of academics experience including HOD, Director in earlier Engineering Colleges in India. His research interests are Telecomm Networking, Mobile Computing, Information Security, Sensor Networks and Soft Computing. He has publications in journals, conference proceedings in his credit. During his academic tenure, he has attended, organized and conducted training programs in Computer, Electronics & Telecomm branches. He is a Professional member of IEEE. He is also a life member of professional societies such as IETE, ISTE INDIA, and CSI INDIA. He has prominently contributed in the governing council of IETE, INDIA.