IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online): 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Self-Reliant Location Privacy Techniques *In* Location Based Mobile Applications

[1] Balaso Jagdale; [2] Jagdish Bakal

[1] Department of Computer Sc. & Engineering, G H Raisoni College of Engineering,
RTM Nagpur University, Nagpur, India

[2] Professor, Department of Computer Engineering, Principal, S.S. Jondhale College of Engineering
Mumbai University, India

Abstract: Tiny hardware of global positioning almost fitted in every mobile device these days which is carried by humans, animals, vehicles and for that matter, any moving objects. Based on this feasibility of location in devices, many location aided applications are being used these days. But revealing location to various service providers to be part of quality of service, pose threat of location privacy. Privacy has got many dimensions including laws, social attitude, governance, commerce and technical. Authors have tried to address above parameters to balance privacy. Revealing location to distributed, trusted parties is also a threat. That is why users' device should be reliant to work for self-motivated privacy. Our proposed work provides location privacy to the LBS users without using any third party for anonymization. Cloaking mechanisms are suggested with different parameters such as location plaintext in group, location noise, and encryption. Customization is studied that progressively increase the privacy levels. The user can use any of the module depending on the context it is requesting the LBS. Prototype is demonstrated with LBS system and Mobile emulations and delay, communication cost, privacy strength is measured and analyzed among these parameters variation.

Keywords: *Geoinformatics, Location Privacy, Mobile Computing, Location based services, Cloaking*

1. Introduction

Recent technologies allow to measure and track location of object .Few of the technologies such as GPS gives location in the form of Latitude and Longitude. Positioning systems collect huge amount of this sensitive location information as time progresses. Mobile users naturally needs location aided services e.g. finding 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. Commercial services are available from many providers. To name few, like Google, Microsoft, Apple, Uber are already providing enterprise level services. 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. Revealing location could make adversaries possible different types of attacks. There could be following categories of privacy:

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

Based on different classes of Location Privacy there are different techniques introduced:

1. Anonymity Based Technique: This provides solution for the identity based and path based location privacy. This technique allows individual to be unidentified.
2. Muddying Based Technique: In this technique, location information is tinted but retains attached with mobile users' identity. Method is based on damaging position information for the defense of location privacy.
3. Policy Based Technique: First regulation is decided about location disclosure. That is policy access matrix or policy access control list is designed. Policy based tools are powerful, flexible but not comfortable for user community to understand. Moreover, for large number of users, it becomes complex and uncontrollable.

2. Related Work

Amongst the techniques K-anonymity technique [1] can be seen as a state of the art where you are indistinguishable amongst numerous other objects. K-anonymization refers to hiding one's identity among K-1 other users in the same

cloaking space. 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. Spatio-temporal model [2] is the traditional model of privacy based on K-anonymity principle. But it has got its own advantages and disadvantages, which are as follows. Advantage is that message perturbation causes pseudonymization of message. Hence, Identity is never revealed and user is hidden against k-users hence difficult to identify the linking of previous path to identify subject. But among disadvantages, trust is on single anonymization server and for larger value of K, privacy is better. Authors [3], describes personalized anonymity method for guarding location privacy. Mobile users can modify privacy requirements with K change. It balances between degree of privacy and Quality of Services and it is free from location distribution attack. But it suffers from more computational resources as it can support K-anoymity only up to K=10. Moreover, searching in graph is costly and if the life time expires, query cannot be answered. In paper [4] authors have suggested to treat anonymizer as cloud storage, which just help client encrypted storage. Actual filtering is at client for quality of service. No third party required but it assumes that users should trust on storage server like Amazons ec2/ec3 on storing private data and if user colludes with one of the storage server for getting information about another user, then it is a threat for privacy. Chow and Morkbel [5] introduces peer cloaking technique, where static mobile members help as service providers.

It is proactive way and on demand consumption of communication cost but it involves long response time. Prevention of location based identity reference of users, who issue spatial queries to LBS framework, has been proposed by Kalnis and others [6]. Without disclosing query source, translations based on the well-known K-anonymity notion is used to compute exact responses for variety and adjacent neighbor hunt. Ghinita et al. [7, 8] have suggested not to share private query information with others, and alternatively suggested ways to protect security. Earlier, Samarati and Sweeney [9, 11] have suggested privacy preserving techniques in information systems and data mining, temporal and spatial dimension are not extensively studied. TeodorIulian et al. [12] discussed adding noise in location information whereas Mokbel [13] suggested peer to peer technique of privacy and addressed issues but delay, cost and privacy strength need to be studied through different angle. Reza et al. [14] have demonstrated usage of mobile crowd sourcing baser anonymization in collaborative environment which is a motivating factor to further study privacy without anonymizer. In our earlier work [15], related to location privacy, we have suggested broadcast protocol which is stronger in its own way, but requires resources and regulatory control to practice such applications. Chunhui et al. [16] have proposed algorithm for interchange and joining anonymity groups to preserve privacy of user in client side environment. Availability and feasibility is demonstrated by authors experimentally. However, commercial, technical, legal challenges are not addressed by authors.

First, most of them trust a single anonymization agent (Trusted Third Party). This allows storing users' location information with their identity, which makes the TTP the single target of attacks by malicious parties. Second, the single agent is a performance bottleneck since it needs to process all updates and anonymization. Finally, they do not consider attacks on user's trajectory i.e.in case of continuous queries the user can be easily identified because user's successive cloaking regions disclose moving trend of user.

3. Proposed Research Work

Location based services have become ubiquitous everywhere. This leads to storing and investigation of a massive amount of information as a part of research study. Before achieving the goals of LBS there is need to balance Information and Privacy. With the use of LBS user can get highly personalized information .Location based services are categorized into following, Navigation, Tracking, Information, Billing, and Social Networking. If Location Based Service Provider is not managed properly, it could jeopardize users.

Problem definition: Performance analysis of various collaborative approaches for location anonymization from security perspective, user's need perspective and value of service perspective. Prime objective of this research is to study delay, cost and privacy while not depending on third party server for location anonymization.

Scope: Scope of this project is to measure the performance of the system while executing the project design techniques. Also, measure the Quality of Service based on the anonymity achieved.

Objectives**:** The objective of project is that, our design should provide the users location privacy while users are using location applications. The locations shared among the users to achieve collaborative effort to anonymize location are secured. The design is flexible enough so that user can choose the approach according to his security requirements

Architecture of the system
Basic Scenario of requesting LBS is shown in figure 1.

1. User U sends request to LBS Provider with following information: User Identity (ID_u), Query, Location (Latitude, Longitude).
2. LBS Provider P replies to request of U.

Privacy Problems:
1. When P knows that user is in shopping market, so it can send to U lot many advertisements.
2. From consecutive queries, P is able to track the user.
3. P can leak the users' location information to any untrusted third party.

Two main Solutions proposed in Literature are:
1. K-anonymity approach. Here position of the user is masked under several k users.
2. Querying P with inaccurate position. Which is nothing but distortion of the real location.

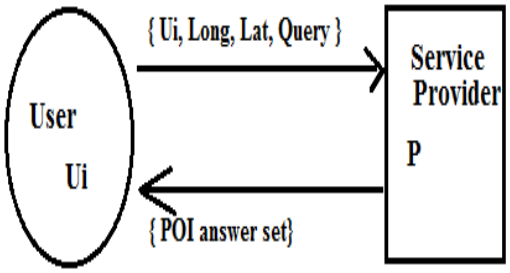

Figure 1. Basic Architecture for LBS query

Proposed work follows concept of achieving location privacy without using Trusted Third Party for anonymization. Below figure no 2 shows the basic scenario of our proposal. This proposal is based on computing the centroid of k users (including requesting user U) and requesting LBS provider with the same. This centroid is the inaccurate location but gives the expected results to the user. Also this calculated centroid can be used by other K-1 neighbors for their use.
Computing a centroid: Once user receive location information of K-1 neighbors', U calculates the centroid Ū with following equation no 1.

$$Centroid\ \bar{U} = \left(\frac{\sum_{i=1}^{K} long(xi)}{K}, \frac{\sum_{i=1}^{K} lat(yi)}{K}\right) \ldots\ldots (1)$$

Where, Location (long (xi), lat (yi) is the location of mobile user Ui.

Self-Reliant Different approaches

A) Plaintext Location exchange among K Users

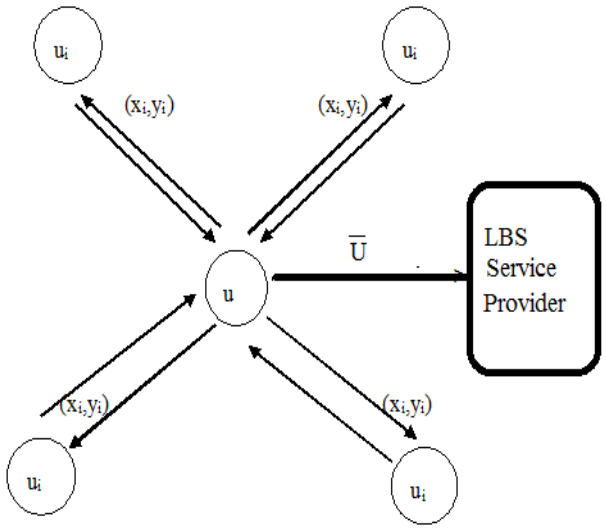

Figure 2. Basic Scenario for proposed architecture

In this module u receives location from k-1 neighbors and calculates centroid. Using this centroid (anonymous location) u requests LBS provider and also sends same centroid to other neighbors also. This module is useful when neighbors are in list of friends.

B) Noisy Location exchange among K users: Noise + Plaintext

Drawback of above module is that we assume that there is mutual trust between K-1 neighbors and user U. But in many circumstances mobile users favor to hide their actual location from other users. The above module fails to accomplish this requirement. Hence, each neighbor adds Gaussian's noise to their actual location. Then it calculates the centroid from noisy locations and request to LBS provider. Unlike plain approach, this approach is resistant to mischievous users because he does not know the location of mobile users but the concealed one.

C) Noisy location exchange among K users with chaining topology: Noise+ Plaintext+ Chaining

This scheme can be overcome to drawback of Module 2 Gaussian's noise with null average when user is not changing his location. As chaining is performed , requester user has to reveal his location to neighbor user hence that first neighbor is the only person who knows the exact location and if he is trusted then this scheme is more secure and less time consuming. Here the only point of attack is first neighbor.

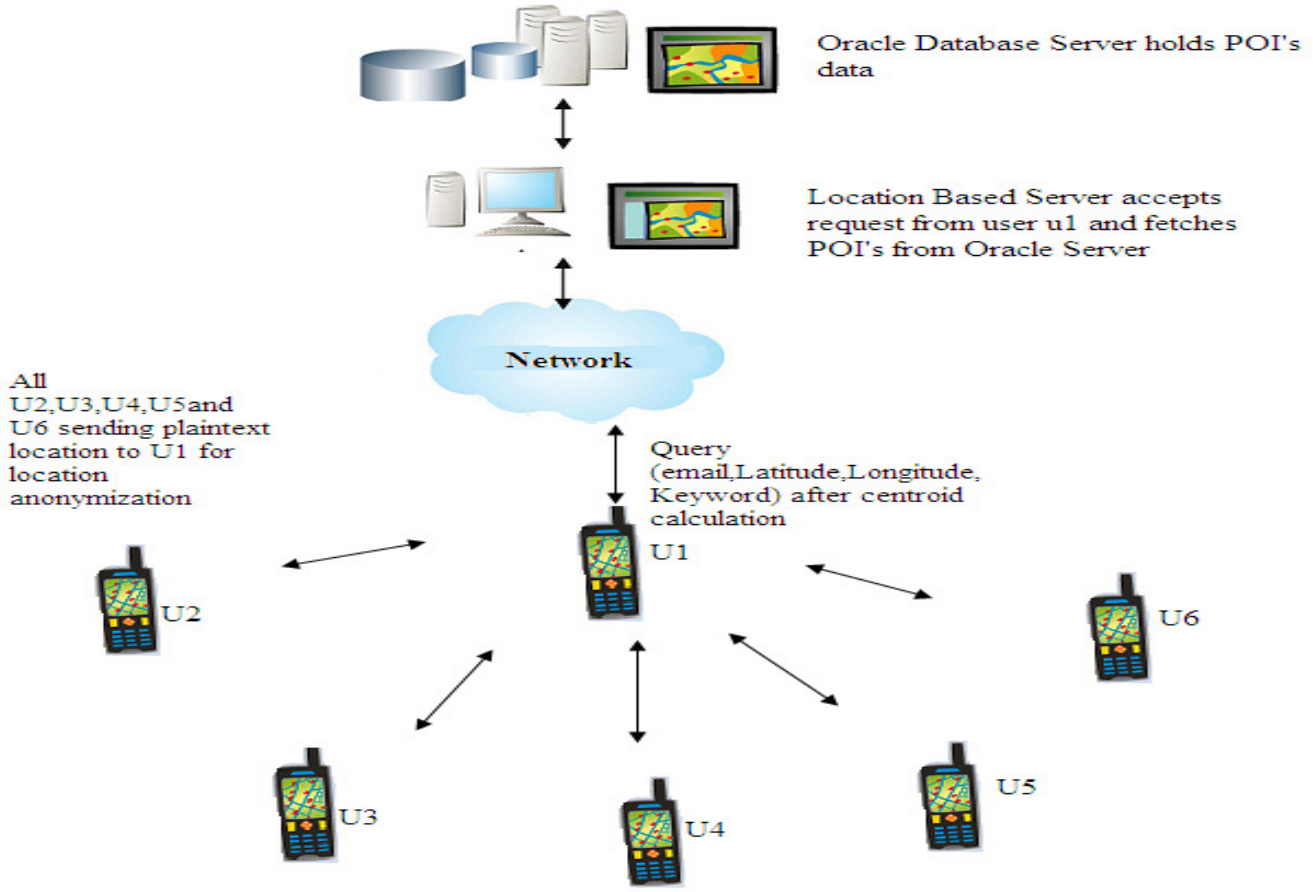

Figure 3. Module1: all users are sending their locations as plaintext.

D) Encrypted location exchange among K users: PH +Noise +Plaintext

Repeated use of Gaussian's noise can cancel added noise. To avoid this limitation it is essential to prevent user U from perceiving noisy values of neighbors. This module uses public key homomorphism for processing encrypted data.

E) Encrypted location exchange among K users with chaining topology: Chain +PH+ Noise+ Plaintext

This module introduces arbitrary chaining among mobile users, which regulates the order in which communications will be exchanged. Due to this message exchanging, it is not centralized.

Specific Requirements:

A GPS enabled mobile phone/device is primary requirement for the proposed architecture. These mobile phones possess Location Based Service which makes use of GPS for retrieving its actual location for querying LBS as per the user request.

An untrusted LBS provider is next requirement for this proposal whose task is to provide services to users.

A group of K mobile users U = {U1, U2, U3, U4, U5,…, UK} where Ui € U and left over K-1 mobile members act as neighbors. Neighbors are collaborating in calculating anonymized location.

Networks: There are two kinds of networks used in order to locate requesting user and for interacting with other users.

Fixed Network: Assumption is made that mobile users are capable to discover themselves by using a stable network.

Ad hoc Networks: Assumption is made that mobile users are competent to create their own ad hoc network with additional mobile users in U or also link with current one.

We assumed that LBS mobile users are capable to find their location information and other K-1 neighbors in their covering range. The covering range can be defined by the available K users. The radius depends on that assumption only.

Security Requirements:

The security required for proposed work is configured in terms of total number of K neighbors amongst which user want to hide his location and at least space L^2 where these neighbors may be dispersed. The accuracy of anonymization depends on number of k users and area in which they are distributed. The value of K & L depend on the population density in which users are located.

Finding K-1 neighbors: Once security requirements are fulfilled users must able to find K-1 neighbors. Subject to number of mobile users into their covering range, following situations could occur:

- There are no users: If there are no neighbors in the given area user cannot proceed further steps.
- There are less than K mobile users: If we consider K = 5. Scenario is U1 is in contact U2 and U3.Where U3 is in contact of U4 and U5. In this case U1 can contact only U2 and U3 only. To accomplish K=5 user U1 can take help of U3 for finding U4 and U5.
- There are K users or more: Here k neighbors can be effortlessly discovered. In this case, if there are additional than K neighbors say K' then mobile user is capable to choice number of neighbors between preferred K and K'.

4. Implementation

Experimental Setup**:** In this section, experimental setup and implementation of four techniques is presented. This research works has been implemented in Java technology with J2ME, J2SE and JEEE. The setup required to establish the LBS server, mobile-Ad-hoc network, wireless access point for making connection between wireless devices (mobile phones) and switch to connect all networks together.

Diagram in figure 4 shows the actual setup that is needed to accomplish our task. It is expected that all mobile devices in particular area are connected to each other to form a Wi-Fi ad-hoc network. We assume that connection establishment and software deployment is preliminary requirement here. Also, LBS server and database server are connected to each other via 8 point switch. That switch in turn connected to Access point to create a hybrid network.

As shown in figure 4, we set up our experiment work. The switch has been used to connect the two servers LBS application Server and Oracle database server as well as one Access point. Here we have created our own network with simulated mobile devices on Laptop. All emulator instances on laptop first will connect to each other through Connector .As connector is present on LBS Server machine each instance is communicating with another using Wi-Fi access point only. As shown in above architecture diagram in figure 4, there are multiple neighboring users collaborating each other for location anonymization.

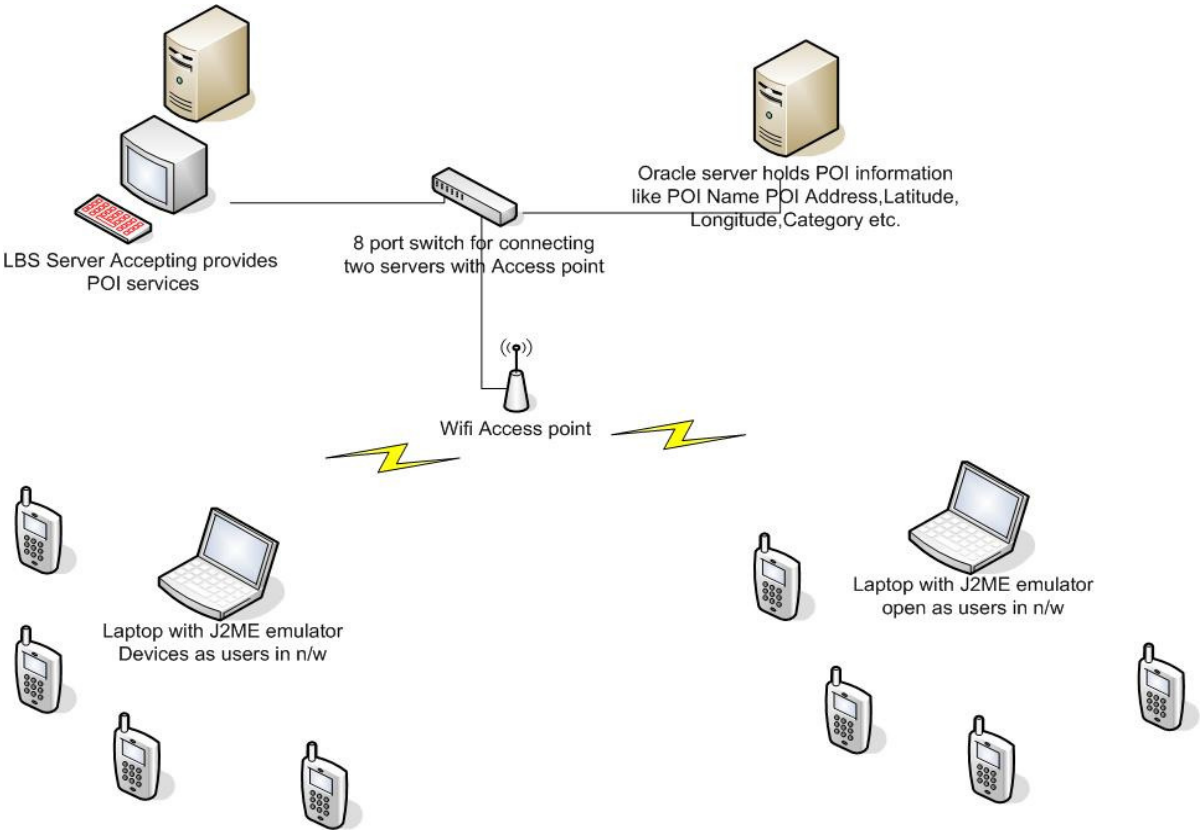

Figure 4. Experimental Setup for our research

The anonymized location is then send to LBS Server. System consists of four sections as follows.

1. LBS Server (J2EE)
2. Oracle Database 10g
3. Connector(J2SE)
4. Mobile Devices (J2ME)

LBS Server: User who has location based facility in his mobile is going to query to LBS server to find out nearest POI with respect to his location. LBS server accepts the user location in the form of Latitude and Longitude, his email address as user identity and keyword for search. Here we assume that user is sending his filter option to LBS server. Instead of providing bulk poi's around him he can restrict them by his choice (e.g. if user want to search for ATM then he does not need Hotel, Hospital poi's).
We have used Java servlet technology for LBS server implementation. The servlet with name PassToLBS accepts userid, latitude, longitude, and keyword. This separates the values from given input stream and sends them to next class.

Database Design: The Oracle database has been created for storing POI's. There are two tables with name **POI_TABLE** and **POI_CAT_TABLE**. POI_TABLE holds the columns such as: POI_ID primary key, POI_NAME, POI_ADDRESS, POI_CAT_ID, POI_LATITUDE, POI_LONGITUDE, POI_ALTITUDE. POI_CAT_ID is the foreign key belong to POI_CAT_TABLE.
POI_CAT_TABLE holds columns such as : POI_CAT_ID (primary key), POI_CAT_TYPE.POI_CAT_TYPE contains poi's category such as atm,bank,Hospital,Clinic,College,School,Restaurant,store,theatre,malls etc.
We populated POI database with 86975 poi records in Pune city.
Connector (J2SE): The concept of project revolves around the TTP-free location anonymization. We assume here as all users have access to Wi-Fi city network. Actual Wi-Fi city network is not possible to set up due to limitations. Hence we have simulated the Wi-Fi Access point as Connector.
We have provided connector some functionality such as message broadcasting .Also it can work upon chaining topology, forwarding message to all mobile devices connected to it. The Mobile devices will be the emulators in J2ME 3.0 sdk. Java socket programming has been used for its implementation.
Mobile Devices (J2ME): We have used Java TM ME sdk Platform 3.0 for mobile application development. Sender class has been used to send the latitude and longitude over the connection stream to Connector and connector will then forward to another user. Client has been created to collaborate the other user who wants to request to LBS user with anonymized location.

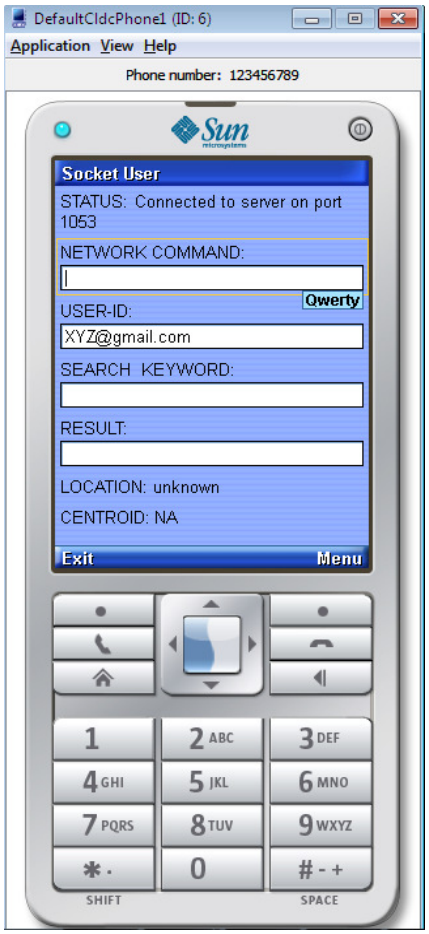

Figure 5 Mobile emulator as Mobile device with GPS facility

Scenario Implementation
The assumption here is that. All users are connected to each other before initiating request for location information. Connector plays role holding connection to all k-users.
First scenario (Requesting plaintext locations): User initiates the request for getting location of k-users for location anonymization. User U initiates the communication with message "get". This is broadcasted by the connector to all other k-users. Once get string is received on the connection, other neighbors reads that and sends their locations to that user. Then user fairly calculates centroid and request LBS server for POIs.
Second scenario (Requesting noisy locations): Other users in Wi-Fi network do not trust the user U, hence neighbors will not send their exact location but they will add Gaussian's noise in it and then send. The Gaussian's noise has property that when we addition of Gaussian's noise (i.e.

while calculating centroid) gives addition zero i.e. it get cancelled. Hence, neighbors can secure their exact location from untrusted user U. but the problem with approach is if neighbors do not change their location then continuously collaborating in anonymization then the noise get cancelled and the actual location of his can be revealed.

Third scenario (Requesting noisy locations with chaining topology) This scenario is same as second scenario only difference is that instead of broadcasting the 'get' message the chain is formed among all k-users. User U sends its location to next user. Next user in chain adds his location into that similarly the sum of locations is forwarded into chain and finally requester user receives the sum and calculates the centroid. Using this approach only requesting user's location will be revealed to first neighbor only.

Fourth scenario (Requesting encrypted locations) By knowing the limitations of Gaussian's noise we have used Encryption Homomorphism. Where each neighbor encrypts its noisy location using LBSs public key and then send to requester user U .Encryption homomorphism is nothing but doing some mathematical operations on encrypted values without knowing the actual plaintext.

Fifth scenario (Requesting encrypted locations with chaining topology) In this scheme, we have used chaining topology instead of broadcasting. Same topology has been used in third scenario. Only difference is user send encrypted location instead of simple noisy location. In this scheme it is provided that each user first encrypts his location and add it with the received location and forward it to next user.

5. Results and Analysis

We will analyze above mentioned techniques (methods) on different scenarios.

A) **Average End to End delay for every scheme:** The total time required from request initiation for locations to getting results from LBS has been computed with respect to validate which scheme takes more time .Below table shows the results we have taken for end to end delay for 10 users i.e. (1 requesting user and 9 neighbors)

If we analyze graph in figure 6, it is clear that time goes on increasing as each user puts some value in it for his security. At first point, every user has trust on every other user hence there is no more overhead before sending locations to requester user. At second point, for Module 2 here no user trusts each other hence adding some Gaussian's noise in it so that it is hiding himself from requester user , as a result the requester user will get the same centroid as in Module1 because Gaussian's noise comes to zero after addition of all users location. Hence, there is slight increase in time. At third point, users are adding noise and instead of all users sending their location to requester user they are forming chain. At point 4, user have encrypted their noisy locations and sending them to requesting user hence for encryption some time has required hence increase in time. At point 5, same as previous but chaining is done and time got increased.

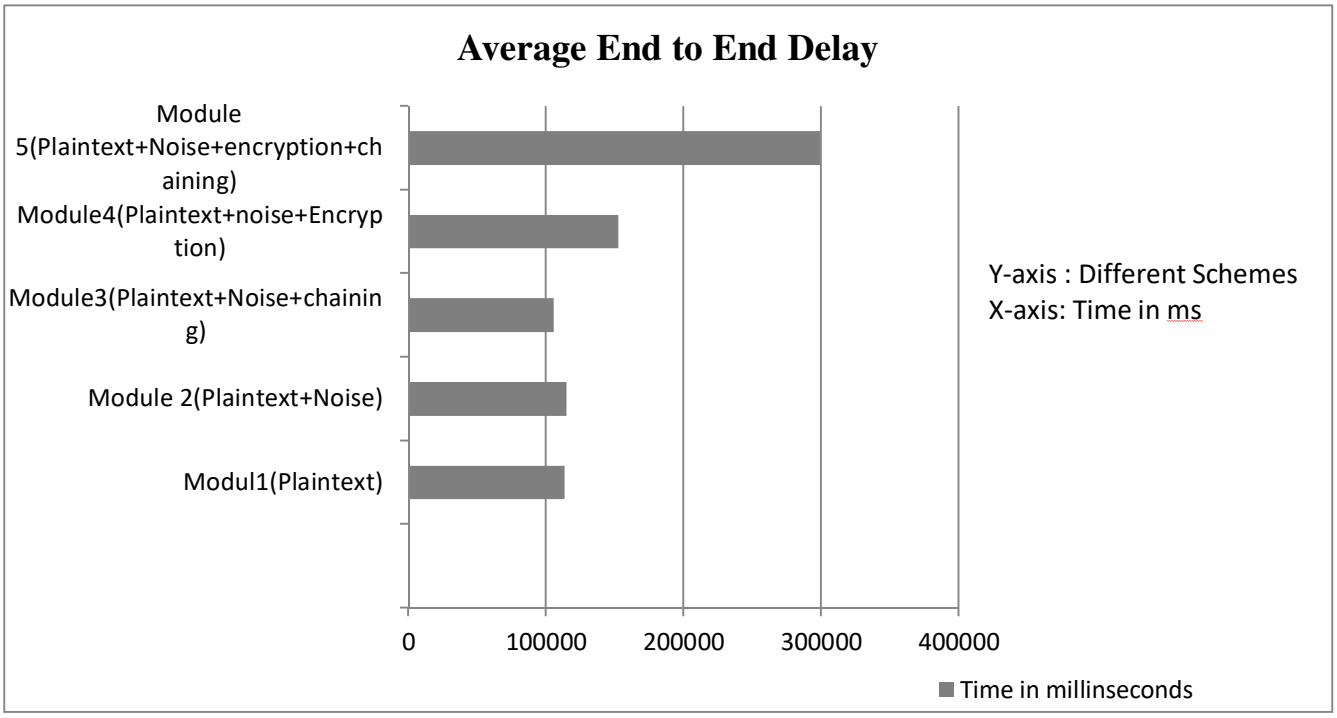

Figure 6 Service- Average End to End delay

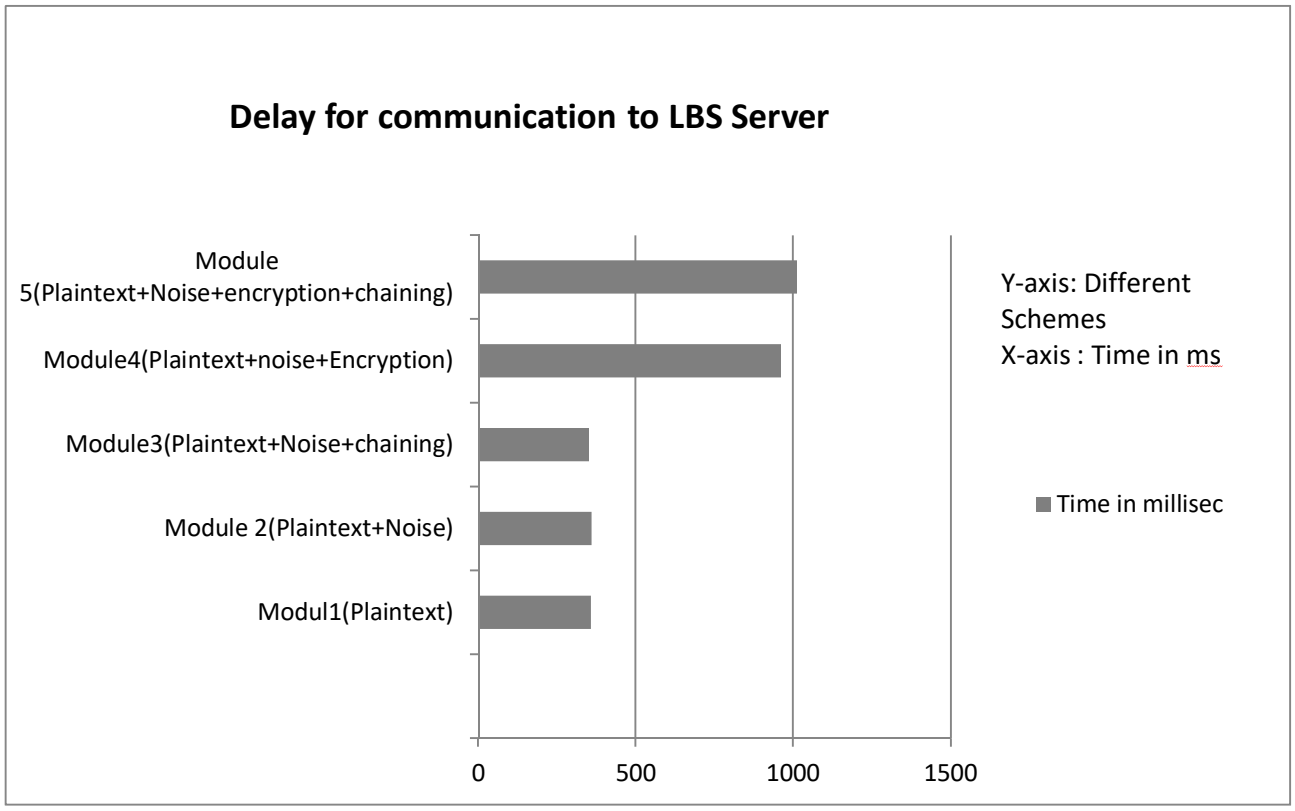

Figure 7 Average delay for actual communication to LBS server for POIs

B) **Average delay for actual communication to LBS server:** The time required for querying LBS server for POIs after the distributed anonymization has been computed here. Below table shows the different schemes vs. time required in milliseconds for 10 users i.e. (1 requester user and 9 neighbors). The graph in figure 7, shows the time variation for request and reply for LBS server for querying nearest POIs.

It is seen that for first three schemes time required is same because LBS does not need to do anything but just executing query and giving results back. For last two schemes the locations are encrypted hence before querying to oracle server LBS has to decrypt the locations calculate the centroid and then giving results back. Hence, time taken is more.

C) **Query results accuracy With Centroid calculation:** Figure 8 shows the time delays for communication from end to end. Also, if we see in the literature we have found that no one has talked about the accuracy of query results with respect to method of anonymization. But, here we have calculated the Query results accuracy with respect to three schemes, First when neighbors are collocated near to requesting user .Second when neighbors and requesting user are uniformly distributed. Third, when neighbors are far away from requesting user as he did not find nearby.

D) **Anonymization / Privacy levels:** To check with the number of neighbors the requested user got with the annonymization they achieved. This not only depends on the number of neighbors it got but also the distance and the direction in which neighbors got distributed. Figure 9 shows different neighbors against the distance of centroid from the original location.

If we take average of the all values we see the value we will get is 0.05972 which says that permissible location anonymization would be 0.05972 or we will say it as threshold value for location anonymization.

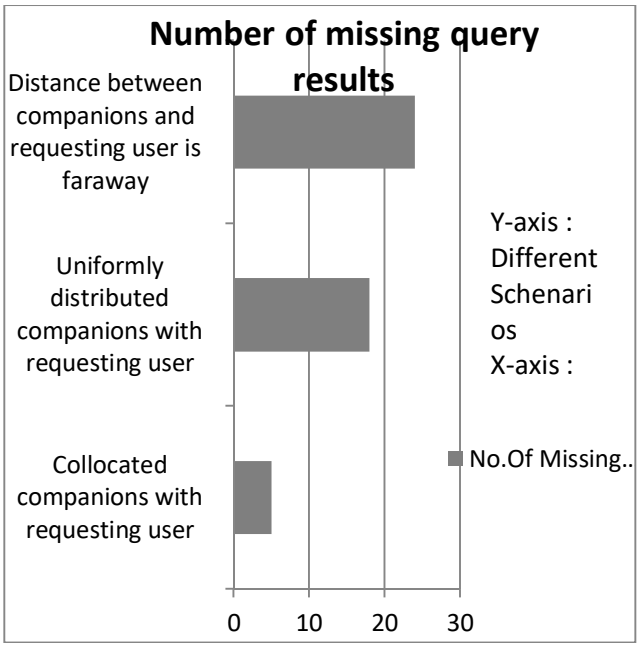

Figure 8 No of missing query results with the Distribution of neighbor

Hence, centroid difference in range of 0.04 - 0.06 is satisfactory from results perspective as well as anonymity perspective. With this if we get the centroid below threshold value we will get good results but if there centroid is too low from threshold then there is possibility of disclosure of original location. Along with the same if value exceeds the threshold we get anonymisation but the results will be bad.

6. Conclusion and Future Scope

Our location privacy technique improves the existing approach of location privacy from security perspective as, it does not rely on Anonymizer, It is distributed hence no problem of bottleneck at single point, It is strong against the conspiracy of a malicious mobile user and a location service provider.

This work is implemented in different modules that they really need according to users need. By using this cloaking technique, the mobile users can safeguard their position privacy even if they are stationary and not moving.
Irrespective of TTP based or TTP-free, finding out K-neighbors within range is a challenge. Till now, we assume that we need K-neighbors to satisfy our requirements. But,

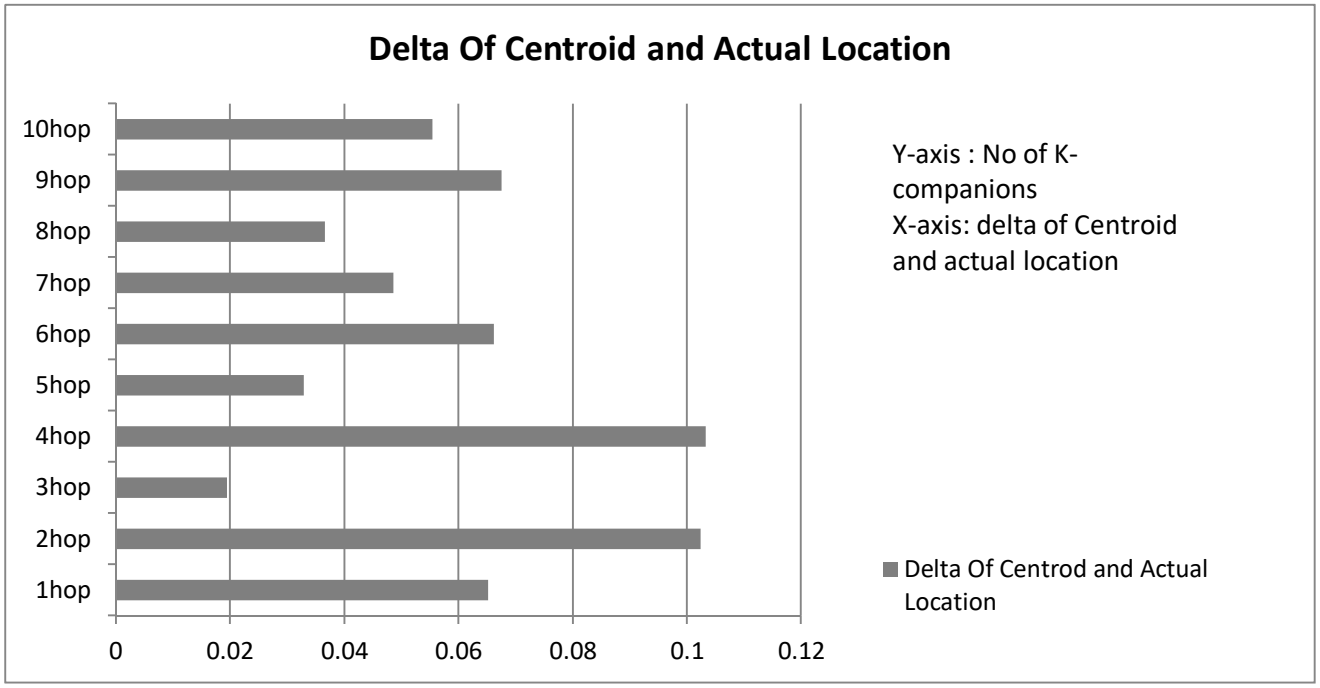

Figure 9 Graph of number of neighbors vs. Delta of Centroid and Actual location.

if there are no neighbor found, we need to generate K-neighbors with the help of Haversine distance method. Cloaking is customized based on context, where we can pick up different schemes based on Processing delay, Communication cost, Privacy level. This has been shown with empirical results as shown in the graphs.

References

[1] Agusti Solanas, Antoni Antoni Martınez-Balleste, "A TTP-free protocol for location privacy in location-based services", Journal Computer Communications archive Volume 31 Issue 6, April, 2008

[2] M. Gruteser, D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking." Proceedings of the First International Conference on Mobile Systems, Applications and Services, 2003.

[3] B. Gredik ,L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms", IEEE Transactions on Mobile Computing.(2008)

[4] Krishna P.N. Puttaswamy and Ben Y. Zhao, "Preserving Privacy in Location-based Mobile Social Applications", ACM 978-1-4503-0005, February-2010.

[5] C. Chow, Mohammad F. Mokbel and Xan Liu. "A Peer-to-Peer Spatial Cloaking Algorithms for Anonymous Location-based Services", ACM-59593, November 2011.

[6] P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial queries", IEEE Transactions on Knowledge and Data Engineering-2008.

[7] G. Ghinita,P. Kalnis, A. Khoshgozaran, "Private queries in Location based services Anonymisers are not necessary", Proceedings of the ACM SIGMOD international conference on Management of data, 2008.

[8] Gabriel Ghinita, Panos Kalnis, Spiros Skiadopoulos. "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems", ACM Transaction-978-1-59593, 2007.

[9] P. Samarati, "Protecting respondents identities in microdata release", IEEE Transactions on Knowledge and Data Engineering, Vol. 13, No. 6, pages 1010-1027, 2001.

[10] Paillier, Pascal. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." Advances in Cryptology. 99. Web. 20 Oct. 2009.

[11] P. Samarati, L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression", Technical report, SRI International, 1998.

[12] TeodorIulian Alecu, Sviatoslav Voloshynovskiy and Thierry Pun, "The Gaussian Transform of Distributions: Definition", IEEE transaction on Computation and Application.2006.

[13] M.F. Mokbel, Chi-Yin Chow, "Challenges in preserving location privacy in peer-to-peer environments" in Seventh International Conference on Web-Age Information Management Workshops.China.June 2006.

[14] Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and Jean-Pierre Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014.

[15] B N Jagdale, Bakal J W, "Controlled Broadcast Protocol for Location Privacy in Mobile Applications", International Conference on Information Security and Privacy, ICISP, Pages 782-789, 2015.

[16] C. Piao, Changyou Zhang, et al. "User privacy protection for a mobile commerce alliance", Elsevier Journal on Electronic Commerce Research and Applications Vol. 18, Pages 58–70, 2016.

Authors -

First Author: Balaso Jagdale received the DIE Diploma in Industrial Electronics from Govt. Polytechnic Latur and 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. He has publications in journals, conference proceedings, and books. 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 also associated with Govt. committees, University faculty interview- Subject Expert in Pune and Mumbai University. He is Professional Member of ACM and life Member of CSI, IETE, ISTE INDIA.

Second Author: Dr. Jagdish 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