Designing Anonymity Server based on K Optimal Principle for Privacy Preserving Protocol

Mr. Y. S. Amle, Prof. Dr. S. S. Lomate, Prof. R. A. Auti

Abstract—**There is need to secure mobile phones locations by privacy frame work which utilizes K optimal principles. This improves the location position and tracking ability of Cell phones. Most of the time quality of service cannot be provided because K no. of users may not be available at the time of request. This motivates to create dummy requests at real time, to assure K principle. Another motivation is to split additional load that occurs on Location Based Services (LBS) for adding Anonymization Server (AS) in between Mobile Station (MS) and LBS. To find out nearby location like banks, hotels etc. An algorithm that process mobile request using K secrecy with variety of considerations and different parameters like real world traffic volume data and dummy mobile users generated practically by mobile objects generator to achieve K optimal principle. By this temporal clocking problem solved as there is no waiting request.**

Index Terms— **Anonymization Server, K-anonymity, Location Based Services, L-diversity, Mobility, Mobile Station, Privacy**.

I. INTRODUCTION

By using Cell phone capabilities like GPS and multimedia, Location based services are improved. Location based service (LBS) applications are take the geographic location into consideration. Examples of location based services are Transit Genie, Next Bus, and Google Latitude [1]. Generally user submits a request to some location based server and receives a response from LBS. A typical request from a user includes location criteria in the form of «id, time, location(x, y), query». With untrusted servers the privacy and security of an individual may be leaked to adversaries. Several reports are available where GPS devices were used to find out user locations [3, 4]. Knowledge of location may guide to tracking or unwanted advertisements sent to your mobile device.

There are several architectures that are considered for privacy aware location based services. These architectures are peer based trusted third party, and client-server. In the peer based model clients directly with each other peers. In the client server architecture clients communicate directly with the LBS by submitting a request, the LBS then returns a response directly to the client [10, 11]. The intention of the client is to cloak each other in order to satisfy the K anonymous principle.

The trusted third party model utilizes the concept of a middle-ware between the mobile user and the LBS. System sometimes refers to the middle-ware as anonymization server (AS). Cell phone requests are first sent to the middleware, the request is then cloaked into a region with the spatial and temporal tolerance and it refer to this as a region request. The request is then cloaked with other user's region request. It refers to it as an aggregate region request.

Work is focused on the trusted third party architecture design. Location privacy in location based system is to prevent adversaries from locating cell phone users past or current locations and the time the locations where visited. System used the concept of k-anonymity [8, 9] and L-diversity [7] to prevent request linking. Mobile users in these frameworks are considered K-anonymous if a mobile user cannot be distinguished from at least K-1 other mobile users in the same region request. The concept of L-diversity ensures that the queries in region request are not homogenous.

II. RELATED WORK

In 2003, Marco Grateser, Dirk Grunwald "Anonymous usage of location Based Services through spatial and temporal cloaking" introduced concept of Location privacy can be achieved by using spatial and temporal dimension of still user. And also focus on sender anonymity, meaning that eavesdroppers on the network and LBS providers cannot determine the originator of a message. The drawback of paper was Communication Privacy Threat.

In 2005, Y. Yanagisarva, H. Kido T. Satoh "Location traceability of user in location Based service" briefly introduced that Location privacy of moving object or moving user but the drawback was in Formalized tree structure that is to locate path from source to destination by considering all possible paths.

Manuscript received December 11,2015.

Prof. Yogesh S. Amle, Bachelor of Engineering in Information Technology, Student, EESCOET, Aurangabad, Maharashtra, India.

Prof. Dr. Santosh S. Lomate has Master Degree and Ph. D. in the field of Computer science and Engineering, Director of Everest Education Society Aurangabad. Maharashtra, India.

Prof. Rajesh A. Auti, Bachelors and Master's Degree in the field of Computer science and Engineering, Aurangabad. Maharashtra, India.

In the same year 2005, Bugra Gedik, Ling Liu "Location Privacy in Mobile system: A personalize anonymization model" briefly introduced concept of personalized K-anonymity model for providing location privacy. They developed a Novel message pertubation engine based on Clique cloak algorithm to implement the system model. The drawback of system was that 10 percent of all request messages were dropped and success rate reduced.

In 2007, the researchers Tanzima Hashem, Lars Kulik "Safe guarding location privacy in wireless and adhoc networks". They introduced concept of hiding user identification and position- using K anonymity principle to achieve QoS. The main drawback was if K requests are not available at time of request then user request maybe dropped.

Again, in 2007, Ling Liu "From data privacy to Location privacy" briefly introduced that Location privacy from data privacy. It also introduced a combination of 2 location privacy models that is privacy based and Location based location privacy mechanism (Location K anonymity and Location L-diversity). The main drawback was that how to adequate control the location cloaking process in terms of location K-anonymity and location L-diversity.

In 2009, Christian S. Jensen, Hua lu and Man lung Yiu "Location privacy technique in client server architecture" introduced concept of the features where client can hide its true location among fake locations using dummy based technique and also it is easy to implement as they do not rely on any third party. In this architecture clients communicate directly with the LBS by submitting a request, the LBS then returns a response directly to the client. The pitfall of the system was that it lacks any trusted component in between MS and LBS.

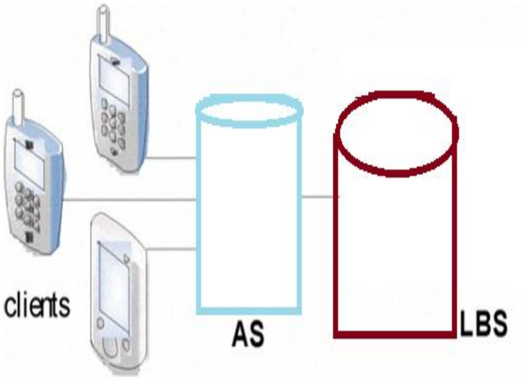

Figure 1: Experimental Setup

In October 2010, Freni, Vicenti, Mascetti, Bettini and Ensen "Preserving Location and Absent Privacy in GeoSpatial networks". They addressed two concept of location preserving and absence privacy in GeoSpatial network. It means if User wants to share photo social network with location, time and listing of who appears in photo. The main issue related was publication delay. Experimental setup including SRS:-

The experiments were conducted on a PC with min 10 GB hard-disk and 512 MB RAM running Windows-7 containing a P6200 Intel DUO 2.13 GHz processor. The algorithms (General algorithm, Cloak LessK, CloakedK and dummies generation) where implemented using jdk 1.6 and the development environment Platform version is Netbeans 7. At the back end we are using MS-SQL server / Oracle for database storage and access. Clients are nothing but Wi-Fi Mobile having Symbian OS used for sending request to finding out nearby desired location.

III. PROGRAMMER's DESIGN

Input: Request Query
In this algorithm the user has to submit a request in the form of Query «userid, msgno, (t, x, y), (dx, dy, dt), P, C» having latitude and longitude dimension for searching nearby hotels, banks, temples etc. Where userid is unique identification number, msgno is message identification number. We are going to use combination of both which is unique for message. (t, x, y) is the temporal and spatial property of the request, (dx, dy, dt) is the spatial and temporal resolution demanded by the mobile user. P is the percentage of privacy desired and C is the request content.

Outcomes:
I) Reply from AS (Anonymization Server)
As a respond for requested query from user for finding nearby locations AS forwarded it to LBS.LBS checks its current position returns reply to AS.AS filter the reply from LBS for precise result and forwarded a path from current location to destination location to user including intermediate stops.
II) It also calculates total distance from user current location to desired location which is a shortest path.
Success definition:
I) Our work guarantees that user personalized request of privacy and Quality of services (QoS) can be satisfied using trusted third party architecture.
II) And also effective work against corollary history attack by utilizing realistic diverse dummies.

A. *Mathematical Model*

Once user submit request query, it contains percentage privacy level (P) as per user demanded. Depending on P we have to map some value of K by using mapping function. We refer it as a transformation phase.

Let n be the total number of users that should be in the cloaking region to guarantee P (percentage privacy). Let P be the percentage of privacy desired by a real user (Ur) Ur: We define k= ceiling (100/ (100-P)).
Intersect and Merge approach: - The figure 2 shows mathematical model for mapping input real user requests from various critical regions with number of dummies needed. When a user submits the required privacy level then we use this privacy level with a value of K in K-anonymity.
If K¡ profileCount then we have to generate K-1 dummies such that k-1 dummies C Ar.

Assume a user Ur submitted a query to the AS with a privacy requirement corresponding to k=5. Let the privacy profile (dummy profile) of Ur be the set
Ar= (Ua1, Ua2, Ua3, Ua4, Ua5, Ua6, Ua7, Ua8) where profileCount=8. In the first cloaking region CR1 we maintain the set (Ur, Ua1, Ua2, Ua3, Ua4). Assume Ur submits another query in CR2 with a privacy requirement corresponding to k=6 we maintain the set (Ur, Ua1, Ua2, Ua3, Ua4, Ua5).

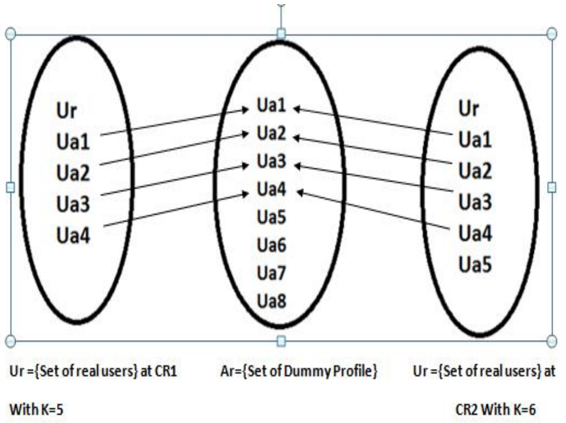
Ur
Ua1
Ua2
Ua3
Ua4
Ua1
Ua2
Ua3
Ua4
Ua5
Ua6
Ua7
Ua8
Ur
Ua1
Ua2
Ua3
Ua4
Ua5
Ur ={Set of real users} at CR1
With K=5
Ar={Set of Dummy Profile}
Ur ={Set of real users} at
CR2 With K=6

Figure 2: Mathematical Model

If Ur submits another query in CR3 with a privacy requirement corresponding to k=7 we maintain the set
(Ur, Ua1, Ua2, Ua3, Ua4, Ua5, Ua6).
Observe that CR1 n CR2 n CR3 = (Ur, Ua1, Ua2, Ua3, Ua4).

This means the user has a 1/5 chance of been identified. Clearly, there is a correspondence between the lowest value of k specified by the user and the chance of been detected region. Hence, it helps in reducing corollary history attack.

B. Dynamic Programming and Serialization

In our system, there is a concept of cloaking that is we have 2 approaches: CloakedK and CloaklessK, Here at this point user has to select any one approach and then go for serialization.
Algorithmic Steps of Overall System (Serialization):- algorithm runs on trusted third party Anonymization Server (AS).
1) Request Sending to AS:-
In this phase, User has to send region request to AS. Request contains percentage privacy levels, as per user requirement.
2) Transformation Phase:-
In this phase, as per user privacy percentage is transformed into some value of K by using mapping function.
3) Here, at this point user has 2 options:-CloaklessK and CloakedK.
i) In CloaklessK, Once AS get region request, It immediate generate remaining dummies to achieve K-optimal principle
ii) In CloakedK, Once AS get region request, It will search for more request if K value is not achieved and add it into region request even if it is not satisfied then it will generate remaining dummies and send aggregate region request to LBS.
4) LBS processes on queries and send appropriate reply to AS
5) Finally, as Filters the reply messages for precise results and send it to various users. Realistic time dummy generation, separating real user request from dummy request (Filtering) and intersect and merging methods uses dynamic programming approach i.e. divide and conquer strategy is used.

Realistic Dummy generation Algorithm:-

1) Initialize profileCount to max value of K. The profileCount can be defined as total no of dummy request associated with real user.
2) Read dummy profile by passing userid and msgno and find out total dummies needed.
3) To generate dummies realistically we use here is spatial and temporal properties of real user.i.e. His current location dimensions and current time (t, x, y).

C. Data independence and Data Flow architecture

Data independence part comes into picture at CloaklessK and CloakedK algorithm.

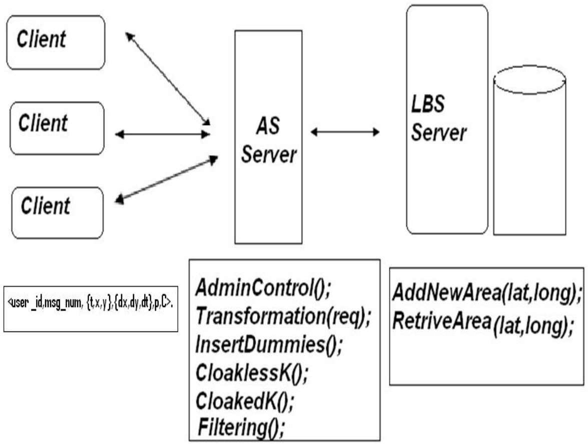

Figure 3: Data Flow Diagram

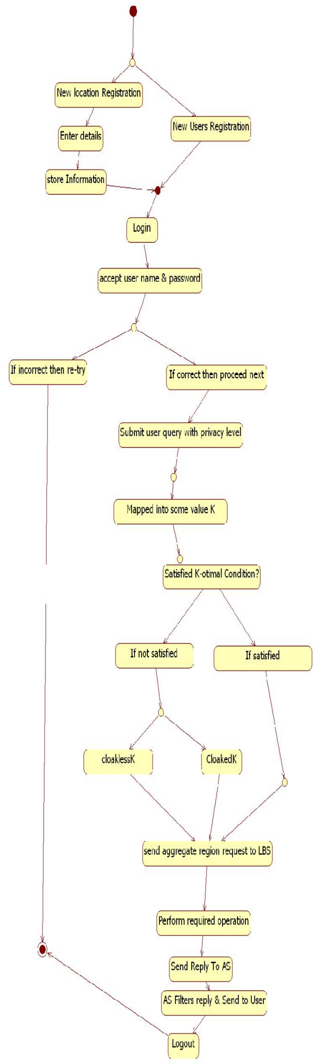
New location Registration
New Users Registration
Enter details
store Information
Login
accept user name & password
If incorrect then re-try
If correct then proceed next
Submit user query with privacy level
Mapped into some value K
Satisfied K-otimal Condition?
If not satisfied
If satisfied
cloaklessK
CloakedK
send aggregate region request to LBS
Perform required operation
Send Reply To AS
AS Filters reply & Send to User
Logout

Figure 4: State Chart Diagram

CloaklessK Algorithm:-
Input:- request «userid,msgnum,(t,x,y),(dx,dy,dt),p,C»
1) Calculate hash value based on (userid,msgnum).
2) Calculate value of K, depending on percentage privacy level using transformation function.
3) Create aggregate region.
4) Insert real user request.
5) Add dummies into real user requests.
6) Send region requests to LBS.

CloakedK Algorithm:-
Input:- request «userid,msgnum,(t,x,y),(dx,dy,dt),p,C»
1) Calculate hash value based on(userid,msgnum).
2) Calculate value of K,depending on percentage privacy level using transformation function.
3) Create aggregate region.
4) Insert real user request.
5) Finding out more nearby requests.
6) If till k-optimal condition is not satisfied then add dummies into real user.
7) Send region request to LSB.
The system data flow architecture is shown in figure3.

A. *Turing Machine*

A simple state diagram showing possible changes in states incorporating multiplexer logic is shown in figure4.

IV. RESULTS

One of the most important evaluation criteria is success rate. The main goal of anonymization server is to maximize the number of user requests that can be added successfully. We can measure the success rate as the ratio of the number of anonym zed request by the total number of individual mobile request. As we are going to add dummies into real requests so there is not at all chances of request drop, So AS server achieves 100 percent success rate.

Another evaluation criterion is the cloaking time. The cloaking time of an algorithm is the time taken to perturb the requests. An algorithm cloaked K provides remarkable cloaking time as compared to CloaklessK. Cloaking time is a performance measure.

The third evaluation considered is the communication cost. Communication cost defined as the number of region request sent to the LBS by the AS for a fixed amount of request. As in our algorithm we are using 2 models: CloaklessK and CloakedK. CloaklessK have fixed communication cost while
CloakedK have much lower communication Cost. If number of requests increases CloakedK provides good results for communication cost.

V. CONCLUSION

1) All queries are given a response, in previous existing System [10] some queries are dropped, so success rate Improved.
2) Spatial cloaking problem solved, as we extends the region to search for K other requests.
3) Temporal cloaking problem solved, as no waiting for actual request by adding dummies.
4) Communication cost reduced as in our algorithm we are using 2 models: CloaklessK and CloakedK. CloaklessK have fixed communication cost while CloakedK have much lower communication Cost. If number of requests increases CloakedK provides good results for communication cost.
5) Corollary History attack protection. References

REFERENCES

[1] http://www.google.com/latitude/intro.html.
[2] R. Agrawal and E. Wimmers. A Framework for Expressing and Combining Preferences. In Proceedings of the ACM International Conference on Management of Data, SIGMOD, 2000.
[3] Federal Communications Commission http://www. fcc.gov/cgb/consumerfacts/wireless911 srvc.html.
[4] S. Mascetti, C. Bettini, D. Freni, X. Wang. Spatial

Generalization Algorithms for LBS Privacy Preservation. Journal of Location Based Services ISSN I748- 9725/ISSN 1748-9733, 2007.

[5] Leon Stenneth Phillip S. Yu Ouri Wolfson,Phillip S. Yu, Ouri Wolfson, “Mobile Systems Location Privacy: “MobiPriv” A Robust K Anonymous System”. 2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing, Networking and Communications.

[6] Lui, From Data Privacy to Location Privacy: Models and Algorithms. VLDB, 2007.

[7] F. Liu, K. Hua, Y. Cai. Query I-Diveristy in Location Based Services. International Conference on Mobile Data Management, 2009.

[8] M. Grusteser and D. Grunwald. Anonymous usage of loyu67ujcation based services through spatial and temporal cloaking. ACM/USENIX MobiSys, 2003.

[9] H. Kido, Y. Yanagisawa, T. Satoh. An Anonymous Communication Technique using Dummies for Location Based Services. Second International Conference on Pervasive Services, 2005.

[10] C. Chow, M. Mokbel, X. Liu. A peer to Peer Spatial Cloaking Algorithm for Anonymous Location Based Services. ACM GIS, 2006. www.tran sitgenie.com

Prof. Yogesh S. Amle, Bachelor of Engineering in Information Technology, Student, EESCOET, Aurangabad, Maharashtra,India.

Prof. Dr. Santosh S. Lomate has Master Degree and Ph. D. in the field of Computer science and Engineering. He has keen interest in the area of data mining, software Engg, fuzzy systems, Neural networks, and has published several papers in National and International conferences and journals. He is also Director of Everest Education Society Aurangabad. Prof. Lomte has more than fifteen years of experience in teaching

Prof. Rajesh A. Auti has Bachelors and Master's Degree in the field of Computer science and Engineering. He has keen interest in the area of software engg, Neural Network. Prof Auti has more than ten years of experience in teaching