DESIGN AND ANALYSIS OF DKRINGA PROTOCOL FOR LOCATION PRIVACY IN TRUSTED ENVIRONMENT

Balaso Jagdale[1] and Jagdish Bakal[2]

[1]Dept of CSE, G H Raisoni College of Engg., RTM Nagpur University, India
[2]S S Jondhale College of Engineering, Mumbai University, Thane, India

ABSTRACT

Originally K-anonymity principle was first used in relational databases to tackle the problem of data anonymity. In earlier protection techniques K threshold is used as personalization factor for mobile users. In case, K users are not present around needy client mobile user, query can be delayed and thus it will not help to achieve the Quality of service parameter. Moreover, authors have adopted methodology that if K-1 additional travelling users or queries are not seen by needy users, dummies are populated in the environment to improve the quality of service. Earlier architectures shows poor usage of K-principle, cryptography and cloaking space, which leads to threat during communication, more communication cost, more computation cost. We present here enhanced privacy model in a trustworthy third party privacy context that employs the notion of K-anonymity. In this work, enhanced algorithms are introduced, that guarantees a success of Location Based Services (LBS) query replies coming back to mobile client. Client sends the query to the anonymization server (AS), where this server cloaks the users with other at least K users. Our novelty in the experiment is that we have introduced cryptography from client to AS, modified earlier algorithms for Ring-Band approach, smart location updates and simulated the scaled experiment in populated cities environment. The AS add the dummies but creates ring-band cloaking area and sends it to LBS server. Cryptography adds some time however ring-band approach reduces communication overhead. We have studied the performance with variation of different parameters. The response from LBS comes to AS with Point of Interests (POIs) along the ring-band. After which AS filters for precise POIs and sends reply to mobile client. With ring-band approach we may also skip the AS and have client to LBS approach directly but without identity protection.

KEYWORDS

Cloaking, Location Privacy, Location-Based Services, Anonymization Server, Trusted Third Party.

1. INTRODUCTION

While using LBS services for different purposes like finding friends, restaurants, café etc., there is a threat for user of losing the privacy. Due to the loss of location, the malicious user can track the confidential information about the respective user. So matured methods are very much in need to protect the location confidentiality of the mobile users as they are requesting LBS Services. K-anonymity principle is a popular veteran technique practiced in location aided services to achieve the privacy of users' current or past location.

There are multiple architectures for the protection of location privacy of mobile user, such as Tier-I, Tier-II, Tier-III, Tier-N. It means Tier I client side cloaking methods are practiced. Tier- I solutions can be implemented with off-line POI databases. Tier II are client server model LBS services, where there is no less scope for privacy as there is threat from Service Provider itself as service providers may misuse users location data for monetary benefits or for marketing purpose.

DOI : 10.5121/ijsptm.2017.6201

In Tier III, we can add trusted server in the client-LBS server path for helping user to remain anonymous. In our paper, we are demonstrating enhanced Tier III model where cloaking is adjusted such that communication cost is balanced. IT is also possible to have N-Tier architectures, where multiple agent servers will have some role to play based on privacy policies and business rules. Idea is do not directly approach LBS for service, but approach regulatory agents or middle trusted servers to cloak users so that directly they are not exposed to service providers.

The research work is further arranged as follows. Section 2 briefs about similar work presented by different authors. Our thought process is also reflected in this section. Section 3 contains details of proposed work including new terms, design, cloaking algorithms and supporting algorithms. In the section 4, implementation set up and prototype simulation output is illustrated. Objective parameters such as performance, privacy and communication cost are discussed and analysed in part 5. And finally, last section summarizes this paper with future scope

2. RELATED WORK

Leon and others have introduced the realistic dummy generations and cloaking algorithms [1]. Their work is based on cloaking help of trusted server for the mobile users' community. They have shown cloaking performance and quality of service of various cloaking algorithms with different population of users. However communication security is not addressed between mobile user and anonymization server. Moreover experimental user population and size of cloaking area does not reflect situation like populated countries. Traditional K-anonymity with application of location privacy has been described by other Authors [2, 4, 5 & 9]. This work demonstrates less about performance and quality of service issues. Gedik presented work for personalized privacy [3]. Taxonomy of LBS applications has been presented by Schiller and others [6], such as push services, pull services etc. Kido and others [7] put forward the theory of dummy location database creation in location based services. The mobile user queries with the dummy positions alongside real position to the LBS for some service. LBS answers with responses to the client for both type of locations i.e. real position and dummy position. It is easily seen that the client will need to filter the responses and drop the responses of dummy positions. More processing or computing is required to be done by client mobile device. As a result, battery power and life is reduced. Even communication cost will be more as many responses are carried towards client device. Author you & lee [8] have suggested privacy for moving tracks using dummies, where dummies are synthetic and not realistic dummies. Kalnis et al. [10] have proposed identity privacy for user who issue spatial queries, based on anonymizer, and other himself has pointed about continuous queries as challenges as it add computing complexities. And collaborative approach benefits are not addressed for identity privacy. Earlier research of privacy is presented by Morkbel and Gruteser [11, 12], where these paper discusses basics of privacy. These methods are easy to implement in today's context, but does not address current challenges of modern threats. Temporal or historical locations are used to create the hiding region before query is sent to the LBS server [13]. Poor side of this work is synthetically generated user data which does not reflect larger densities or user population. Authors [14, 15] continue to experiment K-anonymity based method for personal identity protection as a part of privacy protection. Dataset in this spatial-temporal research is generated and does not reflect real users' characteristics. Yet inference attacks are possible due to non-random process which is accepted by author himself. Ben and other [16] have expressed entropy based dummy selection algorithm to achieve and improve location privacy. Cloaking area size increase assures privacy but at the cost of complexity and computation cost. Ngo and Kim have studied the overhead due to Hilbert curve based privacy in terms of computing and communication cost [17]. They have shown reduction in cloaking area size but not expressed privacy value in terms of reduction of resources usage. Lindenberg et al.

[18] have proposed modified K-anonymity based system for privacy from historical traces. But we feel that such a system is commercially not viable. Haitao and others have used extended TTP [19], entropy based system of privacy, similar to our proposed system and protected query and location privacy of user. Results are encouraging but privacy strength needs to be discussed. S. Patil et al. [20] presented crowd sourcing help for the protection of location privacy without trusted parties. But trust of other users is at stake and need to be addressed. A. Albelaihy and others have presented survey on recent development of location privacy. Even if comparison is done, but there is absence of realization of techniques [21]. We found our self on right track to consider and implement idea of modified and enhanced cloaking.

3. PROPOSED PRIVACY WORK

It is proposed to design and implement anonymization technique, for privacy in Location Aided Services by using K-anonymity principle and realistic dummy user generation as shown by author Leon [1]. We are modifying architecture for cryptography to achieve authentication and privacy. More over cloaking approach is changed to Ring-band cloaking approach and analyzed the computing cost, Communication cost and privacy strength of the system.

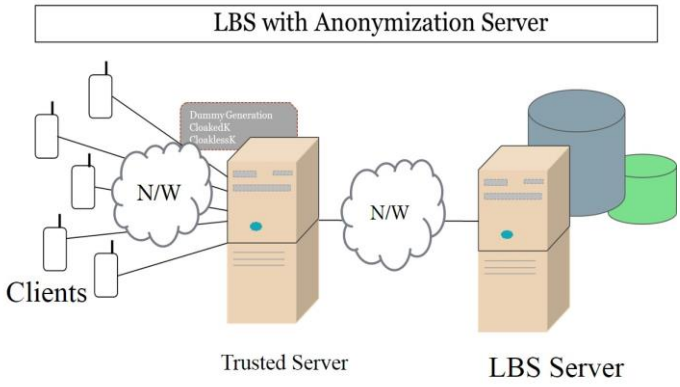

Figure1: System architecture for DKRinga cloaking

Sequence of steps is as follows. As shown in figure 1, mobile clients are members of this system and continuously updates there location to trusted server using RSA public key mechanism. Based on collected location data of all users, trusted server executives DKRinga cloaking algorithm and send cloaking ring to LBS server. LBS server picks up POIs in the ring and sends back to trusted server. Now trusted server filters large replies so as to get nearby POIs of actual query issuer user. These few quality answers are send back with secure RSA public key mechanism to client user.

3.1 FEATURES

We are having the trusted server so that location of user is not exposed directly to the LBS server, thus users location is cloaked by this server. The system proposed in this work is a set of enhanced cloaking algorithms that work on middleware which is also called as an Anonymization Server (AS).

The Mobile user initiates LBS query to AS. There onwards, AS hides or pseudo-generates the identity parameter. AS then hides users' location into a region with K-1 other users in the same area. If K-1 other users are found in the same region, then realistic dummy users are created to meet the threshold. This way, queries are not dropped. We have created the band here and only

band is forwarded to the LBS server to answer the queries. The LBS only fill the POIs in the band. Thus no of POIs will be reduced reducing communication and computing cost required at AS server. POI purifying can be done either at AS or at clients device.

- To implement the scenario a simulator is created, that simulates the Pune map of 2000*2000m.
- The no. of mobile nodes considered to be 500 in this area, which is sending queries to LBS.
- Only the mainstream roads of the city are simulated.
- The simulation can run with 3 levels of Anonymity Threshold that are Low, Medium and high.
- Simulation can be run for different interval and different no. of queries sent for that interval
- After every simulation, different logs are created. Query Processing Log at Client, Cloaking Time Log at AS.

3.2 OBJECTIVES

While study of location privacy is done, it is always important to keep privacy strength as major goal. At the same time, to acquire privacy computing, communication and storage cost is inevitable at different places in the system. Balancing these parameters and achieving privacy is required in such a study.

Objectives are as follows

- To study and improve performance in cloaking (Computing cost)
- To maintain privacy strength
- To reduce communication cost in answering queries
- To introduce cryptography to improve communication path security
- To introduce smart location updates of mobile users who are part of collaboration at trusted server, to be part of cloaking. This reduces computing and communication overhead.

3.3 MODIFIED ALGORITHMS

Normally users leave trace of their positions while they share position for variety of LBS applications. It is easy to infer randomly generated dummy users and their traces as compared to real user's movement. In the cloaking algorithm [1] below, dummies are added in the cloaking area based on spatial and temporal parameter of actual requesting user. The identity profile is taken from look up storage in the form of realistic dummy users. Even requests or queries stored in look up table are dissimilar from every dummy user.

3.3.1 DKRINGAA METHOD PRIVACY

Dummy profile- This is the lookup table file which contains all the users registered with system along with corresponding identity numbers. Each real user is linked with some dummy users, which is referred as profileNo parameter. Initially profileNo is set to maximum value of K. The process of dummy users' addition in cloaking area is performed by anonmization (AS) server for better performance and accuracy.

Algorithm: Ringa-Realistic-Dummy-Generation

```
Begin
    Let mobileUser, NDummies not null
    Set input: mobileUser, NDummies, Q /* Q is a query*/
    profileNo ← 50, count ← 0 , offset
/* dummy users from profile file */
```

```
profile = dummyFile (mobileUser,   NDummies)
    If (NDummies <= profileNo)
            While( count < NDummies)
              t =  Request-getT()+ random()+ offset
              x = Request-getX()+ random()+ offset
              y = Request-getY()+ random()+ offset
              id = profile.nextUserID()
              Q' = Diversify (Q)
              newDummy = createDummy(id,x,y,t,Q')
              Add-DummeyProfile-File(newDummy)
              count++
            EndWhile
     EndIf
     Else return
End
```

3.3.2 PROCESS

Algorithm set the userId, no of dummies and Query Q. 50 number of dummies considered as maximum count for a given real user. Then we read the dummies from lookup file where realistic dummies are stored. If no if dummies required are less than profile count then we should start adding dummies in cloaking area. It is also decided to diversify the query Q such that each dummy user will send different query Q'. Spatial and temporal parameters are updated for real user with randomness and offset. We then generate new dummies and record it in the collection.

3.3.3 ANONYMIZATION TECHNIQUES

The two Anonymization algorithms used here are Ringa-CloakLessK and Ringa-CoakedK. The main advantage of these algorithms is in any case the query is not dropped, since to satisfy the K value in K-anonymity, dummy users are generated.

Algorithm: Ringa-CloakLess-K

1. input: Urequest <user_id, msg_number {t,x,y}, P,Q>
2. Search (user_id, msg_number)
3. Transformation (P)
4. createRingCloak(R1,R2,x,y)
5. insertRealUser()
6. AddDummies-ringband (request, request.K-l)
7. SendRegionRequestToLBS()
8. End

Algorithm: Ringa-Cloaked-K

1. input:Urequest <u_id,msg_number {t,x,y},P,Q>
2. hash (user_id, msg_number)
3. Transformation (P)
4. createRingCloak(R1,R2,x,y)
5. insertRealUser()
6. IntersectAndMerge()
7. AddDummies-ringband(request, request.K-1)
8. SendRegionRequestToLBS()
9. End

Different phases of the algorithms in this section are as follows.

Request Submission: When user initiates request for LBS server, user can set the privacy level as required by user.

Transformation: Percentage of privacy level is transformed to the amount of K which is done with mapping function. Mapping function used here is k = ceiling (100/ (100-p)) where p: percentage privacy level.

Perturbation: we form a circular region as per the requirements from the real user. There onwards, create ring band to reduce cloaking area. In fact ring band is created based on spatial properties of real user.

SendRequest: Two cloaking methods are designed and available for user to select as a part of research prototype simulation. First option is Ringa-CloakLess-K and the other is Ringa-Cloaked-K

In Ringa-CloakLess-K, AS gets a LBS request from mobile user. It swiftly produces K-1 fake users in the hidden area and direct the query to the LBS Server.

In Ringa-Cloaked-K, once AS accepts a query, we check if any other queries are similar and cloaked together. There onwards dummies are generated. To finish, if K-1 real mobile users are not the cloaking area, realistic dummies are added in the cloaking area and finally aggregate query is sent to LBS server.

LBS Server executes the query and sends all the POIs available in ring band as compared to whole circular region. So number is reduced but privacy strength level remains at same level. To narrow down for results, POIs are filtered. This filtering process can be implemented in AS or at the client end if client is powerful. If done at client side, even more privacy strength can be achieved. In our setup, the filtering is done on AS and selected POIs are sent to end user, who requested the LBS service.

3.4 DKRINGA PROTOCOL SYSTEM FOR THE PROTECTION OF PRIVACY IN TRUSTED SYSTEMS

This section discusses our novel contributions of DKRingband system and its pros and cons, with reference to earlier work.

DKRingband is not just a cloaking idea in ring, instead it has got multiple dimensions. Idea in ring band is, instead of rectangular cloaking areas, circular areas of cloaking are used. Since mobile wireless communication happens in omnidirectional and in circular distance range, we get maximum natural benefit of searching, counting, finding mobile users. Secondly we are not considering whole circular area, instead we restrict no of users and POIs by erecting a ring band (size can vary), only in the circular band. This leads to good communication and computing cost benefit as compared to earlier rectangular area of cloaking. This is done while keeping marginally privacy strength at the same level. Other dimension of this DKRingband structure is smartly updating users' locations by restricting sampling and mobility speed of user. Slow users will not generate lot of location data and very fast users should not be part of cloaking. Moreover, RSA public system is used for communication security as it is feasible in today's mobile devices. K-anonymity is not our contribution as it is a part of implementation. Selection of threshold value of K is decided based on density of users and POIs. So cities in India, will need larger K values

while as space cities will have small K-value in practice. We have done experimentation in the range from 5 to 25 to indicate privacy very low to very high.

3.4.1 SMART AND SECURED LOCATION UPDATES TO ANONYMIZATION SERVER

DKringa protocol has two important components. First is the smart and secured update of locations to Anonymization server. Secured location updates from mobile users to Anonymization server are done using public cryptography. Smart and secured update of locations by mobile users' upto anonymization. It called as smart, because mobile user does not update the locations required for cloaking done by anonymization server. ssupdate() algorithm run in mobile client and takes smart decisions if it is required to updates or not. Following algorithm is invoked in mobile user client after interval Uit in ms set by the system. Initial Uit is 16s based on the real experience. This is a global Timer for Ui.

DriverRoutinue()

1. Set Sleep Timer Uit = tfix; // 16m
2. While(not end app)
    a. Get Uilong and Uilat from GPS API
    b. Call ssupdate(Ui, Uilong,Uilat);
    c. Sleep(Uit)
3. endWhile;

Algorithm: ssupdate(user Ui, Uilong, Uilat)

1. INPUT- Mobile node / user Ui gets GPS locations. Ui, Uilong, Uilat
2. OUTPUT- Secured Location update for Ui in AS database system.
4. If (firsttime) update (Ui, Uilong, Uilat) return;
3. Let speed SUi = CalculateSpeed(Ui) // Assuming speed varies from 1 to 16 meters/s
4. If (SUi @ standstill) then
    Do not update location()
    Uit = Uit+Delta;
    Return;
5. Uit = (tfix – SUi)X 1000; ms // if 0 set 1 sec
6. update (Ui,Uilong,Uilat)
7. Return

Algorithm update (Ui, Uilong, Uilat)

1. Let Ui-prkey is the private key of Ui
2. Let Ui-pubkey is the public key of Ui
3. Let AS-pubkey is the public key of AS
4. UiCipher = Encrypt(Ui, Uilong, Uilat) with AS-pubkey;
5. Send (AS, UiCipher);
6. End.

3.4.2 RING-BAND STRUCTURE OF CLOAKING RUNS AT ANONYMIZATION SERVER

We are studying the appropriate band size cloaking which reduces filtering time, improves bandwidth utilization. We have assumed initially as bw=100 meters band size. Figure 2 shows the structure and terminology in Ring-band Cloaking.

Algorithm BandFilter(Anwer[])

1. Let POIband[][] is array contains candidate POIs received from LBS server
2. Let Uilong, Uilat and POIi-long, POIi-lat are the GPS points of User and POI
3. For every POI(i) in band
4. Let a = mod(POIi-long) – mod(Ui-long)
5. Let b = mod(POIi-lat) – mod(Ui-lat)
6. Dist= sqrt(a^2 + b^2)
7. If (Dist <100 mtrs) Add-Answer-POI(Answer[], POI-id, POIi-long, POIi-lat)
8. AnswerCipher= Encrypt Answer[] with Ui-pubkey
9. Send(Ui, AnswerCipher)
10. End.

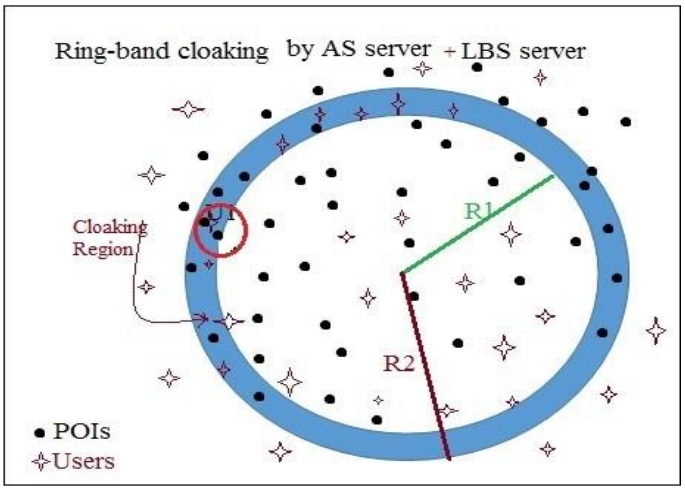

Figure 2: Ring-band cloaking

3.4.3 LBS SERVER ALGORITHM TO SELECT CANDIDATE POIS FROM DATABASE

LBS server algorithm selects the POIs in the ring and only sends those POIs to trusted server for further filtering in order to protect privacy.

Algorithm POI-selection-for-RingBand()

1. Input Cloak-x, Cloak-y, R1, R2; bw= R2-R1;
2. Output Vector of Band-POI[];
3. For every POI(i)
4. Let a = mod(Cloak-x) – mod(POIi-long)
5. Let b = mod(Cloak-y) – mod((POIi-lat)
6. Dist= sqrt(a^2 + b^2)
7. If (Dist < R2) and (Dist >R1) Add candidate-POIs (Band-POI[], POI-id, POIi-long, POIi-lat)
8. EndFor
9. Send(AS, Band-POI[])
10. End.

4. IMPLEMENTATION

A new anonymization technique is proposed in this project which ensures that the user query gets the response. For anonymization, the principal of K-anonymity is used in this project. The problem with previous approaches to K-anonymity is loss of QoS. In that, the query has some

acceptable temporal delay during which the query waits for other K-1 queries to arrive at the server so that server can cloak the K no. of queries and send a region request to LBS. But if K-1 queries do not become available in temporal delay, the query is dropped. This reduces the quality of service. To overcome this situation, the algorithms in this project implements a novel technique of using realistic dummy users to satisfy K value in K-anonymity if K-1 other real users are not available. The two different algorithms implemented here are ringa-Cloaked-K and ringa-Cloakless-K.

Idea of ringa-Cloaked-K algorithm is as follows: When a user sends a request R to AS, it remains at AS for specified temporal delay. If other real user requests arrive at AS in this temporal delay and their location falls in spatial region specified for the query R then they are cloaked. If the cloaked queries satisfy the K value in K-anonymity principle then the cloaked requests are sent to LBS otherwise remaining dummy user requests are generated to satisfy K value and the cloaked queries are sent to LBS. In Ringa-Cloakless-K algorithm, as soon as a user request arrives at the AS, AS calculates K-1 dummy users and cloak the requests and send the cloaked queries to LBS. In both these techniques, despite of using K-anonymity principle, user requests are not dropped because K-1 other requests were not available.

4.1 SCOPE

The main scope of our research project is as follows

- To provide the location privacy using K-anonymity principal and Dummy User Generation.
- A map of 2x2 km of crowded Pune city, India, mainstream roads has been considered for simulation.
- Different Anonymity thresholds can be chosen in the simulator.
- User can also decide the duration of the simulation. For each duration she can alter no. of queries.
- Simulation log is created for every scenario experiment. Query Processing Log at Client, Cloaking Time Log at AS.
- At AS, we can choose one of the two cloaking algorithms i.e. CloaklessK and CloakedK. Depending upon the algorithm chosen the no. of dummy users will be generated.

4.2 DATABASE STRUCTURE

- The Database is designed in Oracle 10G and 2 Tables are created for storing Point of Interests
- **POI_Category_table** is created with following attributes Category_id, Category_name, Counter) and **POI_Table** is created with attributes as poi-id, poi-name, poi-address, poi-lattitude, poi-longitude, poi-category
- POI data / attribute values are generated using a java script which converts data from Google maps API to JSON object in java and then to a csv file.
- The CSV file is then loaded to the database
- There are 35 different categories and around 25000 records available in the database and the database is still populating.
- POI_ID: In this field, the unique IDs for POI's in the database are stored.
- POI_NAME: Here, the name of each POI is stored.
- POI_ADDRESS: In this field, the address of the POI is stored.
- POI_CATEGORY: In this field, the category of the POI requested, eg. Hospital, Restaurant, Shopping Malls etc. are stored.
- POI_LATITUDE: This field gives the latitude of the POI.
- POI_LONGITUDE: This field gives the longitude of the POI.

4.3 EXPERIMENTAL SETUP

To implement this idea, the project has used a client server architectural scenario using socket programming in JAVA. For this, we have used three different PC's having JDK 1.7 and Netbeans 7.0 installed on each PC's.

Client / Simulator PC**:** This PC consist the main Simulator Application. It is connected to the Anonymizer server by using Wi-Fi access point. Anonymization server and the user application communicate using the socket programming.

Anonymizer Server / Middle Server**:** This Anonymization server is setup on a PC. It constitutes the server program code. This server will always be in running state. It can communicate with the LBS Server and the Client Application.

LBS Server: This is a PC, consist of POI database on Oracle 10g. The data of the POI's is collected from the Google Maps. Here, the LBS Server will return the responses to the Anonymization Server through RMI.

Step 1: Select the parameters in the simulation area viz. Interval, No. of Queries etc. This is shown in following snapshot

As shown in the snapshot, the simulator shows some parameters such as simulation area, number of users in the area considered for simulation, the user mobility method. At the simulator we can select different parameters namely anonymity threshold which determines value of K in K-anonymity, Interval, number of queries to be generated for that interval. Start button Click event is used to start the simulation.

Step 2**:** After the simulation starts the different tables displayed are as shown below. The first table, "User Mobility Display" shows the current position of the user. The user move at a speed of 5m/5 sec. Plus Mobility method is used for user movement. In plus mobility method the users' Latitude or Longitude is either increased or decreased randomly. The user mobility display refreshes after every 5 seconds. The second table "Query Request Display" shows the user ids that sent the requests, their time of requests, the point of interest requested by the user. The next table called "Query Response Display" shows the user ids, the time when they get the response, latitude and longitude of the point of interest requested by the user. This point of interest is the nearest one which is found by the AS. The last object shows the directions from the location of user at the time of request to the nearest point of interest requested.

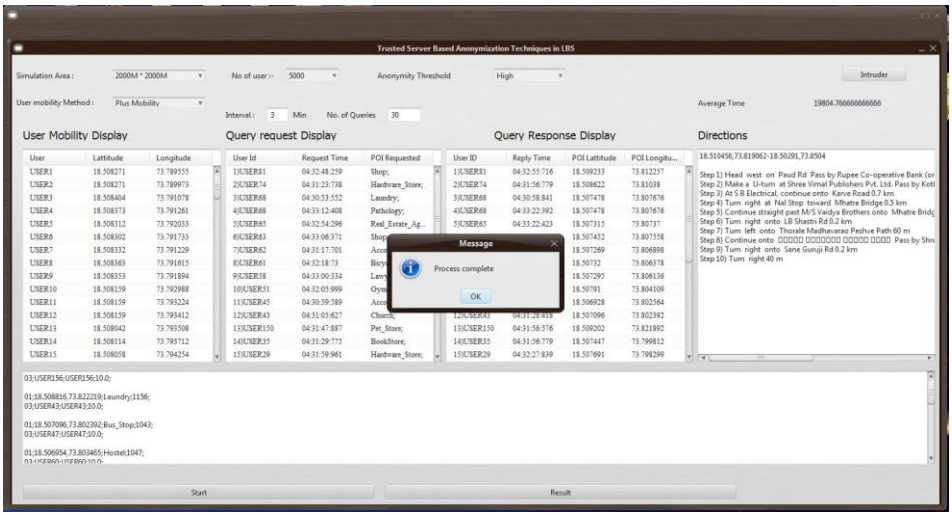

Figure 3: Simulator with Interval =3 min, No. of requests=30, anonymity threshold= High

Step 3**:** After the no. of requests fulfilled the Process Complete dialogue box is shown as shown below. The intruder button shown in the simulator is to generate an adversary request which is in turn blocked by AS. The average time label shows the average time in milliseconds, to process the given queries in given time interval.

Step 4: After the simulation is run by varying the no. of queries to be executed for the same interval, pressing the result will show output in the form of a graph plotted for no. of queries versus average time to process those queries. This also creates a log file which stores the Interval, No. of queries, Average time to process those queries, anonymity threshold and cloaking algorithm i.e. Ringa-Cloaked-K / Ringa-Cloakless-K. A snapshot of result is shown in figure 3. To start the simulation, actually, the first module to be run is location server. Following snapshot shows interface of location server. It displays all the pairs of latitude, longitude between which path is to be found. Next step is to run the module for AS. AS interface lets us to choose one of the two cloaking algorithms i.e. Ringa-cloaked-K and Ringa-Cloakless-K. The interface shows the algorithm specific parameters such as algorithm chosen, source and destination of path, requested POI, real user and dummy users etc.

5. RESULTS AND ANALYSIS

This section discusses performance of modified cloaking and privacy strength analysis.

5.1 PERFORMANCE OF RING BAND CLOAKING ALGORITHMS

Graphs have been plotted between average query processing time and no. of queries for different time intervals and by varying anonymity threshold. Following graphs represent the average query response time for time interval of 1 min and 5 Minute intervals and for Ringa-Cloaked-K and Ringa-Cloakless-K algorithms and anonymity levels low and high.

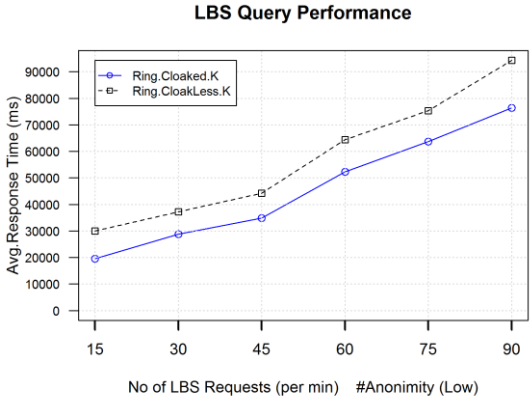

Figure 4: Low Privacy - LBS Performance

From performance graphs it is clear that Ringa-Cloaked-K algorithm takes less average time to process the no. of queries than time required by Ringa-Cloakless-K algorithm to process same no. of queries. This is because the Ringa-Cloaked-K algorithm actually generates less no. of dummy users than Ringa-Cloakless-K algorithm.

5.2 PRIVACY STRENGTH

Graph in figure 8 shows the privacy strength impact on performance. The graph has been plotted for interval 5 min and no. of queries 200 by varying anonymity threshold.

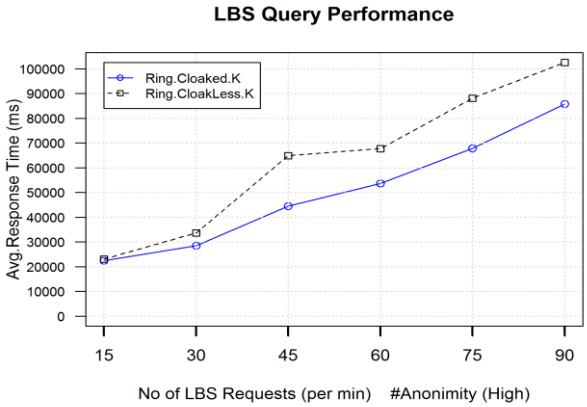

Figure 5: High Privacy - LBS Performance

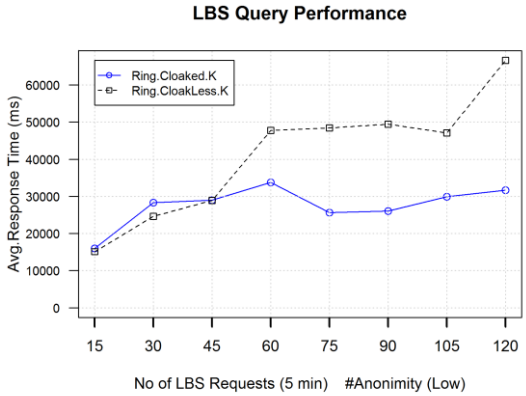

Figure 6: Low Privacy - 5 min Interval - LBS Performance

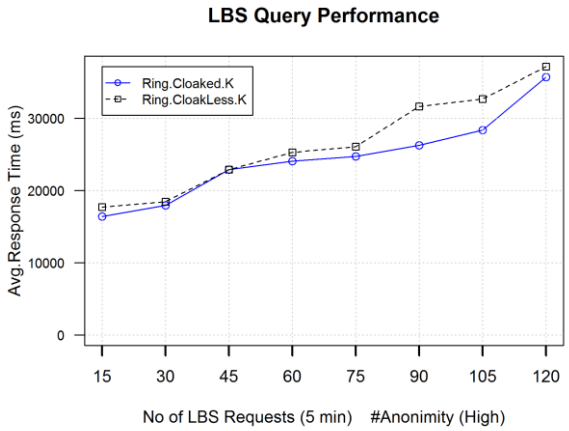

Figure 7: High Privacy - 5 min Interval - LBS Performance

As can be seen that Ring band cloaked-K has better performance than CloakLess-K. But performance remain stable for both the cloaking methods, even if more privacy is demanded by users.

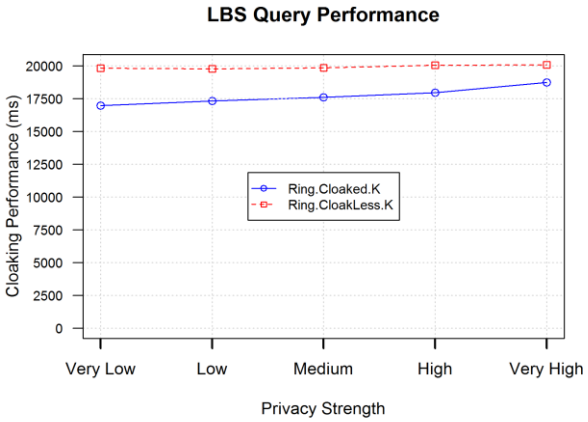

Figure 8: Privacy Strength impact on performance

Higher value of anonymity threshold gives higher value of K and hence better anonymity. If K value increases better privacy strength is provided. If K value increases higher cloaking time is required especially for Ringa-Cloakless-K algorithm since it creates dummies for every individual request. From the graph it becomes clear that as the anonymity threshold increases privacy strength also increases so is the time to process the queries since the time for cloaking individual request increases.

6. CONCLUSIONS AND FUTURE SCOPE

A modified approach to K-anonymity with rectangular cloaking is designed and implemented in this research project which overcomes the problem of query dropping and large regions' requests. This is named as DKRingb and system. It is seen from the graphical results and analysis, that cloaking performance is improved as users and POIs restricted in ring band. This also leads to less communication cost from LBS server to trusted server and from trusted server to client user. The performance of the system is analyzed for different intervals with varying no. of queries for each interval and different anonymity threshold.

The system gives better success rate than previous algorithms since no request is dropped. This is because, if K-1 real user requests are not available for cloaking, realistic dummy users are generated and request is cloaked for both Ringa-Cloaked-K and Ringa-Cloakless-K algorithms. The Ringa-Cloakless-K algorithm takes more time to process a set of queries than Ringa-Cloaked-K algorithm since dummies are generated for every requests. The privacy strength get maintained at approximately same level even if ring band architecture brought in design instead of full circular cloaking area.

This work can be extended with greater map area, either way traffic disciplines, different type of traffic movement patterns and facility given to users to specify spatial and temporal Tolerances. Limitations of this privacy technique is that it relies on strong and reliable networking. Moreover such a system will face many hurdles from regulatory and commercial point of view.

ACKNOWLEDGEMENTS

We are thankful to MIT College of Engineering, Pune and G H Raisoni College of Engineering for the digital library and information technology resources available to conduct this research. Moreover, UG students at MIT contributed for some implementations in java, oracle server and web server setup required for this realisation. We are also thankful for valuable inputs from Mr. Darshankar working in WIPRO, INDIA. These inputs clarified our queries related to latest innovations in the field of LBS applications.

REFERENCES

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

[2] Aris Gkoulalas–Divanis, Panos Kalnis, Vassilios S. Verykios, “Providing K–Anonymity in Location Based Services”, ACM SIGKDD Explorations Newsletter Volume 12 Issue 1, June 2010.

[3] B. Gedik, L. Liu, G. Tech, "Location Privacy in Mobile Systems: A Personalized Anonymization Model", Proceedings. 25th IEEE International Conference on Distributed Computing Systems ICDCS 2005.

[4] Amirreza Masoumzadeh, James Joshi, “An Alternative Approach to k-Anonymity for Location-Based Services”, 8th International Conference on Mobile Web Information Systems (MobiWIS), September 2011.

[5] L. Sweeney, “K-Anonymity: a Model for Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (5), (2002) 557–570.

[6] Jochen Schiller, Agnes Voisard, “Location-Based Services”, Morgan-Kaufmann Pub. ISBN: 1-55860-929-6, 2006.

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

[8] T. You, W. Peng, and W. C. Lee, “Protecting Moving Trajectories Using Dummies”, International Workshop on Privacy-Aware Location-Based Mobile Services, 2007.

[9] P. Samarati and L. Sweeney, “Protecting privacy when disclosing information: K-Anonymity and its enforcement through generalization and suppression”, In Proceedings of the IEEE Symposium on Research in Security and Privacy (SRSP), 1998.

[10] P. Kalnis, G. Ghinita, K. Mouratidis, D. Papadias, “Preventing Location-Based Identity Inference in Anonymous Spatial Queries”, IEEE Transactions on Knowledge and Data Engineering, 19(12):1719-1733, 2007.

[11] M. F. Mokbel, C. Y. Chow, W. G. Aref, “The new Casper: query processing for location services without compromising privacy”, In Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB), pages 763-774, 2006.

[12] M. Gruteser and D. Grunwald, “Anonymous Usage of Location-based Services through Spatial and Temporal Cloaking”, In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MOBISYS), pages 31-42, 2003.

[13] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services", In Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM), pages 547-555, 2008.
[14] P. Zacharouli, A. Gkoulalas-Divanis, V. S. Verykios, "A K-Anonymity model for spatiotemporal data", In Proceedings of the IEEE Workshop on Spatio-Temporal Data Mining (STDM), pages 555-564, 2007
[15] C. Bettini, X. S. Wang, S. Jajodia, "Protecting privacy against Location Based Personal Identification", In Proceedings of the 2nd VLDB Workshop on Secure Data Management, pages 185-199, 2005.
[16] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, Hui Li, "Achieving k-anonymity in privacy-aware location-based services," IEEE Conference on Computer Communications, Pages: 754 -762, DOI: 10.1109/INFOCOM.2014.6848002, IEEE INFOCOM 2014.
[17] Hoa Ngo and Jong Kim, "Location Privacy via Differential Private Perturbation of Cloaking Area," IEEE 28th Computer Security Foundations Symposium, DOI: 10.1109/CSF.2015.12, 2015.
[18] P. P. Lindenberg, Bo-Chao Cheng and Yu-Ling Hsueh, "Novel location privacy protection strategies for Location-Based Services," 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, 2015, pp. 866-870.
[19] Z. Haitao, Z. Lei, F. Weimiao and M. Chunguang, "A Users Collaborative Scheme for Location and Query Privacy," 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Wuhan, 2016, pp.383-390.
[20] S. Patil, S. Ramayane, M. Jadhav and P. Pachorkar, "Hiding User Privacy in Location Base Services through Mobile Collaboration," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp.1105-1107.
[21] A. Albelaihy and J. Cazalas, "A survey of the current trends of privacy techniques employed in protecting the Location privacy of users in LBSs," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017,pp.19-24.

AUTHORS

B N Jagdale received the DIE diploama 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.

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.