A Method of Location Privacy Protection in Road Network Environment

Jianjun Wen[1], *Zhao Li*[1]

[1]Chongqing University of Posts and Telecommunications, College of Computer Science and Technology, Chongqing Engineering Research Center of Mobile Internet Data Application, Chongqing City 400065, China

Abstract. With the widespread application of location-based services, users 'privacy concerns have become the focus of users' attention. Based on the k-anonymity method and the SpaceTwist algorithm, this paper proposes a method of incremental inquiry user privacy protection. The method preliminarily anonymizes the user's location information and points of interest on the client side, On the anonymous server side, combining the road network environment with the latitude and longitude grid generates the minimum anonymous area of random loop, instead of the user initiating incremental inquiry to the location service provider, Anonymous zones ensure k-anonymity for mobile users and road information to protect user privacy. Security and experimental analysis show that this scheme can improve the effectiveness of user query service while meeting the privacy requirements of users.

1 Introduction

With the rapid development of mobile Internet and mobile terminal technologies, location-based services have become a basic function of mobile terminals and are widely used. For example, mobile users can use their mobile phone to check their nearest restaurants, hospitals and gas stations and so on from anywhere.

However, since the user must send his or her location to the location service provider if he wants to enjoy the service, the location service provides greater convenience to the mobile user and has a problem of exposing users' sensitive information. The attacker may cooperate with the location service provider to steal and inquire the user's privacy information and query logs, and may further analyze the user's POI (point of interest), hobbies, place of residence and other private information. For example, when a mobile user queries his nearest eye hospital, the attacker syndication location server provider obtains the location information of the user and the inquiry information, so as to infer that the user is a sensitive group of ophthalmic diseases and push spamming for the user. This shows that user privacy protection is very important.

2 Related Works

In recent years, research on location-based privacy protection of user location has achieved some results, most of which are based on k-anonymity algorithm[1] and SpaceTwist algorithm[2]. K-anonymity algorithm is usually used in the third-party anonymous server architecture. In this architecture, when a mobile user initiates a request to LBS (Location Based Services), it adds k-1 redundant information to its request information, so that LBS cannot identify the user's real request, so as to achieve a certain degree of privacy protection. Location-based privacy algorithms[3-9] used by third-party anonymous service architecture is often based on the assumption that third-party anonymous servers are completely trustworthy. However, in reality, third-party anonymous servers are not completely trustworthy. Therefore, the privacy protection method using the spatial grid[10] and the grid of latitude-longitude[11] is proposed, and they assume that the anonymous server is not completely reliable. Mobile users need to first simply anonymizing their true location, and then sent to anonymous servers. Literature [12] proposed grid privacy protection method to abandon the third-party anonymous server, through the grid pre-divided encryption to handle location privacy issues. Jinying Jia[13] et al in the k-anonymous based on the use of segmentation center method to deal with user privacy protection issues.

SpaceTwist algorithm can get rid of the trusted third-party server, get an anchor randomly in the real location of the user, and then use this anchor to initiate incremental inquiry to the location service provider. However, the location privacy cannot be protected in the case of few users. To solve this problem, Hudson[14] et al solved the problem based on SpaceTwist by expanding user demand area to achieve user k-anonymity. This method may result in the failure of location protection when the information returned by LBS to the user is incorrect information. In [15], k-anonymous episodes are formed by mobile users cooperating with each other, and then uses this anonymous set to initiate an incremental query based on SpaceTwist to the LBS. This method is

* Corresponding author: 894607785@qq.com

not applicable to environments where malicious nodes exist. In [16], a road network-based protection approach is designed, utilizing anonymous trees and min-rings to deal with privacy protection based on road network users. Literature [17] adopts customer-server architecture. Users calculate the upcoming end of the route and initiate the service request to the LBS by replacing the real location with the end of the route. Although this method protects the user's current location, there is a risk of revealing where the user is about to arrive. In a specific environment, location privacy is more exposed. For example, in a network environment, a mobile user usually initiates a query request on a road, and an attacker narrows the scope to a road network. If a mobile user initiates. When there is only one road in the request area, the attacker can easily deduce the exact location of the mobile user. This shows that location-specific privacy protection is more challenging.

Based on the above work, this paper, taking into account the user continuous query, road network environment and semi-trusted anonymous server, in the road network environment, proposes a new method of location privacy protection for mobile network users based on latitude-longitude grids.

3 Related Definitions And System Architecture

3.1 Related Definitions

Definition 1 Grid of latitude-longitude[11]. Use $ID(x, y)$ to represent a unique grid of latitude-longitude. Where x is the latitude for which accuracy is a fraction and y is the latitude for which accuracy is a fraction.

Definition 2 Mobile User Privacy Configuration Function.

$$Qs = \{id, AMIN, Ku, Kp, Lr, Poi, Kr\} \quad (1)$$

Where in id indicates the unique request identifier of the user, and $AMIN$ indicates the minimum anonymous zone set by the user and the location service provider can know the minimum range of the mobile user. The minimum number of mobile users in the anonymous zone is Ku. Kp is the minimum number of different POIs in the anonymous set $Piog\{p_1, p_2, \cdots, p_m; m \geq 1\}$, Lr is the anonymous area contains the least number of roads, Kr is the number of points of interest the user desires to return, and Poi is the POI of the user.

Definition 3 Mobile users request function to anonymous server.

$$Qu = \{id, ID(x, y), AMIN, Ku, Lr, Poig, Kr\} \quad (2)$$

Definition 4 anonymous server request function to LBS.

$$Qa = \{KL - ASR, Poig, Kr\} \quad (3)$$

$KL - ASR$ is the smallest anonymous area for satisfying anonymous needs.

Definition 5 Mobile user location update request function.

$$Info(IDpre, IDcur) \quad (4)$$

$IDpre$ represents the previous grid ID, $IDcur$ represents the grid ID of the current user belongs, this function is used to inform the anonymous server when the grid of latitude-longitude of the mobile user changes.

3.2 System Architecture

This program uses a central server architecture, mainly consists of three parts: Mobile users, information anonymous server and location service provider's server. Mobile users with GPS or mobile base station positioning system to get their own latitude and longitude information function. The anonymizer holds the number of users and road information in each grid of latitude-longitude in its jurisdiction and provides anonymous lookup services to mobile users. The location server provider grasps the distribution of global interest points and provides bulk incremental queries. System architecture and workflow illustrated in figure 1.

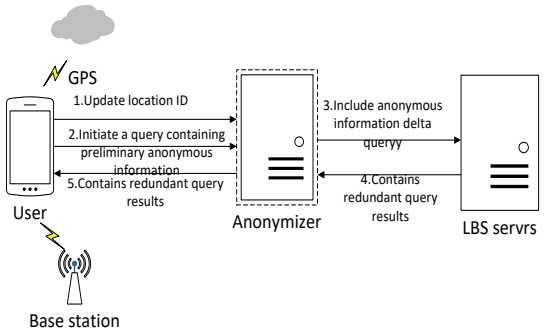

Figure 1. System Architecture and Workflow

In Figure 1, when the location changes, the mobile user needs to initiate a location ID update request to an anonymous server. When a user initiates a location service query request, the mobile user needs to first anonymize the location information and the type of point of interest, and then uses the processed information to initiate an anonymous server request. The anonymous server generates the anonymous area through the privacy parameters configured by the user, and then uses the anonymous area to initiate the KNN incremental inquiry to the location service provider server, and finally returns the requested candidate queried result to the mobile user. After the mobile user receives the returned result, it then filters the returned result.

Mobile users in the entire query request, without providing detailed location information, even the anonymous server cannot get the user's specific location information. At the same time, the user also performs anonymous processing on the types of points of interest, thereby ensuring that the point of interest privacy does not leak to the anonymous server and the location server provider with a certain probability.

4 Road Network KNN POI Incremental Inquiry

In this paper, mobile users first generate anonymity for user privacy through the algorithm of user request information generation. Secondly, the anonymous server

uses minimum anonymous region generation algorithm and KNN incremental query algorithm instead of the user to complete the query request, thereby protecting the privacy of mobile users.

4.1. Problem Analysis

The traditional method[1-10] is usually just randomly add a few redundant points of interest to form a POI k-anonymity in the protection of user points of interest. However, when a user initiates a continuous inquiry, there is a problem of privacy disclosure. For example, if the type of the POI requested by the user is A, the anonymous set formed by the continuous request is {A, B, D, F}, {A, C, G, E}, {A, C, D, H}. When the attacker knows that the user is a continuous query, the attacker can quickly deduce the user's POI is A, so as to obtain the user's POI private information.

The common grid of latitude-longitude method adds the grid information in the anonymous area by extending the radius of the anonymous area. This method will cause the generated anonymous area too large, which not only increases the time cost of the minimal anonymous area algorithm Increased network overhead for KNN incremental queries. As shown in Figure 2, assume that the user is ID (4,3), and set the anonymity to 4. Anonymous servers simply add grids for ID (4,2), ID (4,3), ID (5,2), ID (5,3) when adding nearby meshing to generate the smallest anonymous area and then The circumscribed circles of these four grids serve as the anonymous lowest anonymous area and the dotted circle area. When the anonymous server adopts the radius extension method, due to the fixed extension radius, the extended radius is fixed with the grid ID (4, 3) as the origin, and the extension radius makes the anonymous area contain 4 anonymous users. The generated anonymity is a solid circle area. Compared with the dotted circle, the derivative radius anonymous zone generation method adds extra redundant latitude and longitude grids such as ID (4,4), ID (3,4) and ID (4,5), resulting in the generation of the smallest anonymous zone too large.

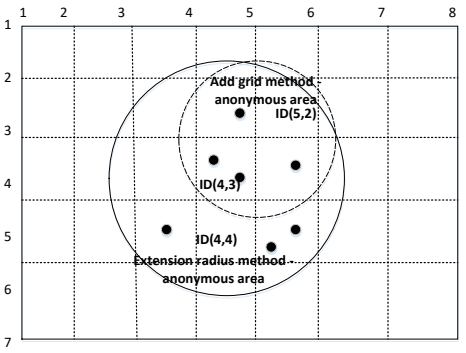

Figure 2. Comparison of the smallest anonymous area

In response to the above problems, this paper uses a random loop minimum anonymous area generation algorithm and user request information generation algorithm to enhance user privacy protection while improving user quality of service.

4.2. User Request Information Generation Algorithm

When a mobile terminal initiates a request to a semi-trusted anonymous center, it needs to perform simple desensitization processing on its own sensitive information and configure related privacy parameters so that the anonymous server can perform personalized and anonymous operations for the mobile user. Based on the original algorithm, this algorithm solves the problem that user's continuous inquiry will expose user's POI. The specific algorithm is shown in Table 1.

The algorithm is mainly used to generate an Poig(anonymous point of interest group) to meet the user configuration and the PoiArry (POI cache array) updates. Before each request, check whether the current request POI exists in the first kp elements of the cache array, and if there exists, directly form an anonymous set of points of interest in the first kp POI in the PoiArry; otherwise, Select kp-1 POI to form the PoiArry with the current query poi, and finally add the Poig to the top of the PoiArry. The user's Poigs are all the same when they are continuously requested, so the attacker cannot parse the user's real POI.

Table 1. requests information generation algorithm

Input: ID, AMIN, Ku, Lr, Poi, Kr Output: Qs

1. Mobile get the real locationID（x,y）;
3.if Poi in PoiArry[0:kp]// PoiArry is a poi cache array
4. Poig = PoiArry[0:kp];// Get the first kp poi, Poig is an anonymous set
5. else
6. Poig.add(Poi); add Poi
7. for（0 to kp-1）// Randomly add kp-1 poi
8. Poig.add(PoiArry[randnumber]); // Randomly get poi in PoiArry
9. PoiArry.remove(PoiArry[randnumber]);//Remove the above random poi
10. end for
11. PoiArry.push_front(Piog);// Add Poig to PoiArry
12.end else
13 .return Qu = {id,ID{x,y},Amin,Ku, Lr, Poig{p_1,p_2 ,…p_{kp}},Kr};

4.3 Anonymous Area Generation Algorithm

After the mobile terminal initiates the query request to the anonymous server, the anonymous server first needs to generate the minimum anonymous zone that meets the user's requirement according to the privacy configuration of the mobile user, and then initiates the request to the LBS instead of the user. This paper random loop minimum anonymity area generation algorithm shown in Table 2.

The minimum anonymity area generation algorithm first uses the latitude and the longitude grid as the minimum anonymity area, and then randomly selects an

expansion direction to increase the anonymous area size by adding the adjacent grids of the current anonymous area clockwise until the user privacy requirements are satisfied. Finally, the smallest circumcircle of this anonymous zone is the final smallest anonymous area.

Compared with Hudson's[15] algorithm, the proposed algorithm transfers the anonymous area to the anonymous server on the fixed network side, thus reducing the computational load of mobile users. Compared with the algorithm of generating anonymous region in the literature [11], the proposed algorithm reduces the anonymous area in the road-intensive environment, reduces the network overhead when computing the cost and incrementing the query. At the same time, the random loop generating method in the algorithm avoids the interest Point uneven distribution of the problem, enhance the quality of service users.

Table 2. Anonymous zone generation algorithm

```
Input: ID, AMIN, Ku, Lr
Output: KL-ASR
1.If (ID.ku > = Ku && ID.lr >= Lr)//Judge road and
user information
2.    KL-ASR = The circumscribed circle of the grid ID;
// KL-ASR is the initial anonymous area
3.else //Expand anonymous area
4.  ASR.add(ID);// To add this grid, ASR is a
transitional anonymous zone
5.    while(ASR.Ku >= Ku &&ASR.Lr >= Lr)
6.     direction = ranm()/4;//Randomly confirm
adding direction, 1 to 4 indicate different directions
7.          for( int i : 1 to 4){// Turn clockwise to add
adjacent grid groups
 8.           for(1 to ASR.Thickness(i)) //Add adjacent
grids in this direction,Thickness (i) is the thickness in
the i direction
9.                    ASR.add(AdjacentIDx(i));
10.                   if(ASR.Ku > Ku &&ASR. Lr > Lr)
11.                       break;
12.                end for
13.                if(ASR.ku > Ku &&ASR. lr > lr)
14.                   break;
15.          end for
16.end while
17.If (KL-ASR.R > AMIN.R)
18.    return KL-ASR;
19.else
20.  KL-ASR.R++ until to KL-ASR.R >= AMIN.R;
21.return KL-ASR;
```

4.4 KNN Incremental Query Algorithm

After the anonymous server generates the anonymous zone for the mobile user, it needs to initiate a query for the mobile user to the LBS. In the KNN incremental query algorithm, the anonymous server initiates a request to the LBS with the KL-ASR as the real location of the user, and receives the detailed data returned by the LBS in turn and calculates the number of each POI in the Poig. When the number of POI with the least number of POI is less than Kr, the location server provider is informed to continue the incremental inquiry. When all the number of POI is not less than Kr, the location service provider is informed to stop the incremental query and end the query. Finally, the anonymous server returns the requested data to the mobile user.

5 Security And Proof

5.1 POI Privacy Security Analysis and Proof

The following will be a detailed analysis of the challenger game model. The model is divided into a challenger C (mobile terminal and anonymous server) and an attacker S (location service provider service).

Challenge C generates a $KL-ASR$ according to the privacy parameter, sends the $KL-ASR$ to S, and selects two types of POI poi_1 and poi_2 in the $KL-ASR$ KL-ASR, and sends them to C. C randomly selects a $b \in \{0,1\}$, C generates a new request Qa according to the system parameters and Qa, Poig in Qa contains poi_1 and poi_2, and sends Qa as the challenge cipher text.

Guess S submits a guess on a, s, if 1 = 2, then the attacker said the success.

Definition 1 If the probability of winning the above challenging game for any LBS does not exceed $\frac{1}{2}+negl()$, $negl()$ is a negligible function, the privacy protection method of this article realizes the privacy type of the mobile user's point of interest.

Lemma 1 A Location-based Privacy Protection Method in Road Network Environment to achieve the mobile user point of interest privacy protection.

Proof From the $\{KL-ASR, Poig, Kr\}$ message sent from C to S, S can obtain the anonymous set of the area where the mobile user is located and $Poig$. S after eliminating redundant POI types, POI only leaves poi_1 and poi_2. And C queries poi_1 and poi_2 using the same query parameters so that the location service provider can guess that the probability of b is at most ½. When C initiates a continuous query, the $Poig$ is the same in each C-Request message at this time, so the probability that S scouts b from each request of C is at most 1/2. Suppose that this consecutive query C is launched n times. Since the content of each guess is the same, the probability of guessing b after n times of guessing is at most 1/2. So S guesses the probability of b is $\frac{1}{2} \le \frac{1}{2}+negl()$.

5.2 Location Privacy Security Analysis And Proof

To ensure the privacy of the user's location, LBS should not be able to obtain the specific road information of the user. The following will be a detailed analysis of the challenger game model. The model is divided into challenger C (anonymous server and mobile terminal) and attacker S (malicious location server provider).

Challenge C prepares the request parameters and then generates $KL-ASR$ and $Poig$ based on the request

parameters. C sends $KL-ASR$ to S, S generates $Rg\{p_1, p_2, \cdots, p_l; l \geq 1\}$ (path set) in $KL-ASR$, and S returns $Rg\{p_1, p_2, \cdots, p_l; l \geq 1\}$ to C. C determines the number n of the exact position in $Rg\{p_1, p_2, \cdots, p_l; l \geq 1\}$, C generates Qa using $KL-ASR$ and $Poig$, and z as the challenge cipher text.

Guess S submits n's guess of $n' \in \{0,1\}$, if $n' = n$, then the attacker said the success.

Definition 2 If the probability of winning the challenge game for any L does not exceed $\frac{1}{m} + \frac{1}{k} + negl()$, where m is the size of an anonymous road set, k is the number of mobile users in the anonymous zone, and $negl()$ is a negligible function, the privacy protection method of this document realizes the user's position Privacy and security.

Lemma 2 A Location-based Privacy Protection Method in Road Network Environment to achieve the Mobile User Location Privacy Security.

Proof From C sent $\{KL-ASR, Poig, Kr\}$ information, S can get to $KL-ASR$ and $Poig$. Both POI and mobile users are k-anonymized. So the probabilities of S's location of road information and moving objects are $\frac{1}{m}$ and $\frac{1}{k}$. S calculates the probability that the number of the road where the mobile user are currently located is at most $\frac{1}{m} + \frac{1}{k} \leq \frac{1}{m} + \frac{1}{k} + negl()$.

6 Performance Analysis

6.1 Lab Environment

6.1.1 Hardware and software

Hardware environment: Intel® Core ™ is-4590 CPU @ 3.30 GHX 3.3o GHz, memory: 8.00GB.

Software Environment: Windwos7 64-bit operating system, compiler environment Java1.6, compiled language using the Java language.

6.1.2 Experimental data

Experiments use Thomas Brinkhoff trajectory generator to generate simulated mobile object data and use it to simulate the movement trajectory of 58905 mobile users in the real traffic network in Beijing urban area as a data set. 23562 POIs were randomly distributed in the map.

6.1 Experiment Analysis

In the simulation experiment, the paper compares the GOLLOR(grid of latitude-longitude of the road) with the OGOLL(ordinary grid of latitude-longitude) method of Jiajinying[15]. The two methods in the location service providers to increase the query, the scope of each inquiry to increase 100m. The minimum anonymous area defaults to 3.14km2. In the OGOLL method, the radius of the anonymous area in the anonymous area generating algorithm extends 200m each time. The center of the anonymous area is within 1km near the grid of latitude-longitude of the user. POI anonymity and road anonymity in GOLLOR are 5 and 10.

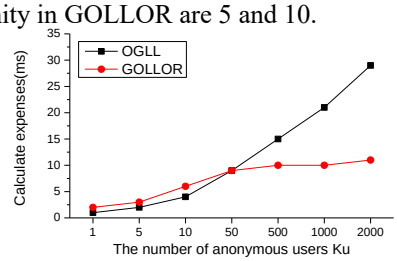

Figure 3. Comparison of computing costs (Ku changes)

Figure 3 shows that the computational cost of both methods increases with the number of target mobile users. Because when generating anonymous areas, both methods add more grids as the number of anonymous mobile users increases, increasing the computational overhead. When the number of anonymous mobile users is less than 50, the computational cost of the two algorithms is quite large, and the computational cost of the latitude and longitude grid method with more than 50 is less computationally expensive. Because the number of redundant grid of latitude-longitude in the anonymous zone generated by the OGOLL method increases with the number of anonymous mobile users, the GOLLOR method does not have a redundant grid of latitude-longitude, so the computational cost of the GOLLOR method is relatively stable.

As can be seen from Figure 4, the network overhead of both methods increases with the increase of Ku. This is due to the fact that both the anonymity of the two algorithms increase with the increase of Ku, so the increase of anonymous area leads to the search radius of the location service provider increasing, resulting in the increase of candidate points of interest points. When Ku is less than 14, the number of POI returned by the location service providers is small because the anonymous area generated by the FF method is smaller and the number of enough POI can be provided in the anonymous area. When Ku is greater than 14, the network cost of the GOLLOR is larger at this time because the candidate set of redundant POI grows too fast in the GOLLOR method.

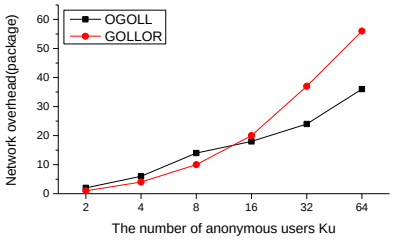

Figure 4. network overhead comparison (Ku changes)

As can be seen from Figure 5, the computational cost of both methods increases with Kr. Because location service providers will increase their computing costs as location service providers search for more points of interest as Kr increases. When Kr is less than 50, the computational cost of the OGOLL method is slightly

higher than that of the GOLLOR method. Because the anonymous area generated by the GOLLOR method is smaller and the number of points of interest in the anonymous area is greater than 50 at this time, the location service provider queries fewer points of interest, so the calculation overhead is smaller. Kr is greater than 50, the GOLLOR method of anonymous area of POI smaller. Because location service providers need to increase the number of queries, it increases the computational overhead.

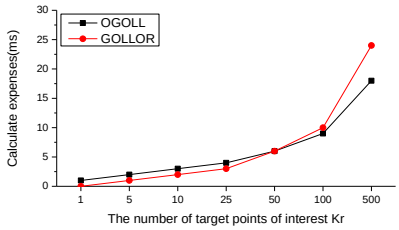

Figure 5. Calculation of cost comparison (Poi change in number)

The experimental results show that the proposed method is not only relatively stable in terms of time overhead but also has less network overhead in practical anonymous mobile users than OGOLL method, which improves the privacy of users and improves the service quality of user queries.

7 Conclusion

Compared with the k-anonymity algorithm, this method replaces the exact location reporting with the latitude-longitude grid, and changes the trusted anonymous server into a semi-trusted anonymous server. Compared with the SpaceTwist algorithm, the anchor point is replaced by an anonymous zone that satisfies the privacy requirement of the user, thereby improving user privacy protection. Compared with OGOLL, the k-anonymity method of road network and POI is introduced, and the anonymity weight of the road is introduced when the anonymous area is generated, so as to further enhance the protection of user privacy. How to protect the mobile trajectory of mobile users by using grid of latitude-longitude in the road network environment[18] will be the issue to be studied in the future.

References

1. Gruteser M, Grunwald D. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, International Conference on Mobile Systems, Applications, and Services. 31-42 (2003).
2. Man L Y, Jensen C S, Huang X, et al. SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services, International Conference on Data Engineering. 366-375 (2008).
3. Bu G G, Liu L. A Customizable k-Anonymity Model for Protecting Location Privacy. Icdcs, 620—629 (2004).
4. Gedik B, Liu L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms, Educational Activities Department, 1 – 18 (2007).
5. Xu T, Cai Y. Exploring Historical Location Data for Anonymity Preservation in Location-Based Services. the, Conference on Computer Communications. 547-555 (2008).
6. Xu T, Cai Y. Feeling-based location privacy protection for location-based services, ACM Conference on Computer and Communications Security, 348-357 (2009).
7. Pan X, Xu J, Meng X. Protecting location privacy against location-dependent attack in mobile services, ACM Conference on Information and Knowledge Management. 1475-1476(2008).
8. GENG Kui, LI Feng-hua, et al.. Proxy-based privacy-preserving scheme for mobile Internet. Journal on Communications, **36**, 25-32 (2015).
9. LIU Shu-bo,LI Yan-min,LIU Meng-jun. Privacy-preserving for Location-based Service over Encrypted Data Search, Hubei Province Computer Society academic annual meeting, 34-35(2014).
10. Pan Xiao, Hao Xing, Meng Xiao-feng. Privacy Preserving Towards Continuous Query in Location-Based Services. Journal of Computer Research and Development, **47**, 121-129 (2010).
11. JIA Jin-ying，ZHANG Feng-li. Incremented KNN inquiry algorithm based on grid of latitude-longitude for location privacy protection. Journal of Application Research of Computers, **31**, 1001-3695 (2014).
12. LI Xiangdong1, ZHANG Shaobo, et al.. Location Privacy Protection Method Based on Grid. Journal of Frontiers of Computer Science and Technology, **11**, 258-1268 (2017)
13. Jia Jinying, ZHANG Fengli. Non-exposure accurate location K-anonymity algorithm in LBS. Scientific World .Scientific world journal. 619357 (2014).
14. Hu Demin， Zheng Xia. SpaceTwist-based k-anonymity incremental nearest neighbor query algorithm for location privacy protection. Journal of Application Research of Computers, 33, 2402-2404 (2016).
15. Pingley A, Yu W, Zhang N, et al. CAP: A Context-Aware Privacy Protection System for Location-Based Services, IEEE International Conference on Distributed Computing Systems. 49-57 (2009).
16. XU E Jiao,LIU Xiang-Yu, et al. A Location Privacy Preserving Approach on Road Network. Chinese Journal of Computers, 34, 865-878 (2011).
17. Zhou Chang ， Ma Chunguang ， Li Zengpeng. Privacy-preserving method for KNN query in road networks. Journal of Application Research of Computers, 2016, 262-265 (2016).

18. Ayong Ye, Yacheng Li, Li Xu, Qing Li,et al. A Trajectory Privacy-Preserving Algorithm Based on Road Networks in Continuous Location-Based Services, IEEE International Conference on Communications. 1-4 (2017).