International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.1-12
http://dx.doi.org/10.14257/ijsia.2015.9.2.01

A Novel Location Privacy Preservation Method for Moving Object

Xu Zhang[1], Ying Xia[1] and HaeYoung Bae[1,2]
[1]*Chongqing University of Posts and Telecommunications, Chongqing, China*
{zhangx, xiaying}@cqupt.edu.cn
[2]*Inha University, Incheon, South Korea*
hybae@inha.ac.kr

Abstract

Location privacy has been a serious concern for mobile users who use location-based services to acquire geographical location. Spatial cloaking technique is a well-known privacy preserving method, which blurs an exact user location into a cloaked region to meet privacy requirements. In this paper, we propose a new semantic privacy preservation method rely on the well-established k-anonymity and l-diversity privacy metrics for semantic cloaking. We also define a representative cloaking region which helps in communication cost reduction caused by user movement. Experimental implementation and analysis exhibit that our proposed method renders good performance in efficiency and scalability. We also show that our proposed method outperforms the existing privacy preservation method by effectively enhance privacy against various adversaries.

Keywords: *Privacy Preservation, Location-based Service, Spatial Cloaking, Moving Object*

1. Introduction

The advances in wireless communication and mobile positioning technologies have resulted in increasingly popularity of location-based services (LBS) in recent years, which also bring a considerable attention in privacy protection. Location based service is a type of service where the information is provided to user with geographic locations. How to protect users' privacy against potentially compromised LBS providers and attackers are of vital importance to existing systems.

Researchers have long been aware of the potential privacy threats associated with LBS, and a lot of promising work has been conducted concerning how to protect location privacy [1-5, 26]. Existing research are drawn on two major types of LBS-related privacy : *query privacy* which refers to user's private information related to query attributes, and *location privacy* which refers to user's private information directly related to their locations [4]. Numerous privacy metric and scheme have been proposed in LBS privacy protection community including [1, 4]:

- *Query Privacy Metric* —— *k-anonymity* is the most popular metric used for LBS query privacy protection, which makes a location indistinguishable from at least *k-1* others [5]. Location entropy stemming from Shannon's entropy is used to quantify the information an adversary can obtain from location updates [6].Ubiquity, congestion and uniformity proposed in [7] exhibit another way to generate an enhanced anonymity query answer set.
- *Location Privacy Metric* —— Depending on how the entropy is defined, location entropy can also be used as a location privacy metric [8]. Expected distance error was

ISSN: 1738-9976 IJSIA

used in [9] to measure how accurately an adversary can estimate a user's location, while Earth mover's distance (EMD) was used in [10] to measure the safety of a cloaking region.

- *Privacy Protection Scheme* —— Policy-based scheme defined the rule for both service providers and users to follow which protect privacy. Trusted anonymization server-based schemes [5, 11] adopted a general architecture that user access LBS service via a trusted server, which blur a user's exact location. Mobile deviced-based schemes [10] is a practical and ease deployment approach, which has advantages over trusted server-based approach. Private information retrieval (PIR) [13] can prevents any type of location-based attacks, however it incurs significant computational overhead on the server side and imposes stringent requirements on LBS server deployment.

A straightforward and generally adopted method in privacy protection is spatial cloaking, which proposed to blur a user's exact location into a cloaked region that satisfies the user specified privacy requirements [5-6, 12, 14-16]. In this work, we proposed a novel method with two phases: (I) *single-user cloaking* and (II) *multi-user cloaking*. Query issuers initialize his cloaking region with the consideration of semantic locations nearby during phase I. Then, user sends his initial cloaking region to neighbors and starts to search peers around and process the multi-user cloaking phase. Users' location related privacy are preserved during both these two phase from both server and neighbor users. We also define and generate a novel representative cloaking region (RCR) in *multi-user cloaking* phase, which helps in communication cost reduction avoiding frequent update caused by user movement.

We conduct a series of experiments to evaluate the performance of our proposed algorithm with several famous works. Experiments are implementation on a modified version of the well-known road network simulator [17]. Experimental results exhibit that our proposed method is efficient in terms of various metrics including cloaking region size, cloaking success rate, privacy level, and effectively reduce communication cost caused by frequent update of users' location.

The remainder of the paper is organized as follows. In Section 2, we review the previous work in location privacy preservation. System architecture is introduced in Section 3 and then the semantic spatial cloaking algorithm is described in detail in Section 4. Finally we show our analysis and experimental results in Section 5 and draw a conclusion in Section 6.

2. Related Work

Recently, various privacy-preserving techniques for location privacy have been widely studied based on several concepts: *privacy policies*, *false locations*, *space transformation* and *spatial cloaking*.

Spatial cloaking techniques rely on *k-anonymity* concept and *cloaking granularity*, which blurs a user's location into a cloaked spatial area that satisfies the user's specified privacy requirements. In terms of system architecture, existing cloaking technique is the most popular privacy preservation method that supports many environments setting including *centralized* [11, 18-20], *distributed* [21-22], and *peer-to-peer* [15, 23] approaches, it also renders good performance in *snapshot queries*, *continuous queries* and *trajectories* [15].

Casper [11] is built based on *k-anonymity*, which resides on a trusted server. It proposed to use an incomplete pyramid structure to maintain users' location thus lowering both location update and cloaking costs. *CacheCloak* [24] is another method also relies on trusted anonymization server architecture, which achieves real-time location privacy protection without loss of location accuracy from LBS service provider perspective. *CliqueCloak* [20] provides a personalized *k-anonymity* model in which users can adjust their privacy level of anonymity to obtain a cloaking region. *Feeling based cloaking* method proposed in [6] use the entropy and quad-tree to measure a cloaking region. P2P-IS-HL-CA [23] is the only peer-to-peer cloaking method, which reduce communication overhead by *information sharing scheme* (IS), overcome network partition problem by *historical location scheme* (HL), and avoid center-of-cloaked-area privacy attack by *cloaked area adjustment scheme* (CA). However, none of the above work considers semantic location and thus cannot avoid similarity location attack [10]. To our best of knowledge, SemGraph [10] is the first research, which deals with semantic cloaking with a graph based on Earth Mover's Distance (EMD).

Table 1. Summary of Privacy Protection Scheme

Approach	Central Server	Mobile Device	P2P Support	Query Privacy	Location Privacy	Semantic Cloaking
CliqueCloak	○	×	×	○	×	×
Casper	○	×	×	○	×	×
CacheCloak	○	○	×	○	○	×
Feeling-based	○	×	×	○	×	×
P2P-IS-HL-CA	×	○	○	○	○	×
SemGraph	○	○	×	○	○	○
Ours	○	○	○	○	○	○

We summary some important cloaking method in Table 1 and indicates several privacy issues not well studied in previous work in next section. Before describing our method, we first give our system architecture in Section 3.

3. System Overview

As it is shown in Figure 1, we design our system architecture with a trusted anonymization server between location based service providers and mobile users. There are 5 main steps for a user to issue a query and obtain answer. Mobile users are expected to obtain location information through GPS or communication networks. Also, it can share location information with neighbor peers. Be aware of that, when user shares location with neighbor peers, it should not be an exact location. We propose to share initial cloaking region between users, which is generated in the *single-user cloaking* phase. This helps us to share information between users while avoiding leak important location information to adversary users. Another advantage of this architecture is that the trust server does not have to anonymize requests independently, but it can instead perform a bulk anonymization on several requests.

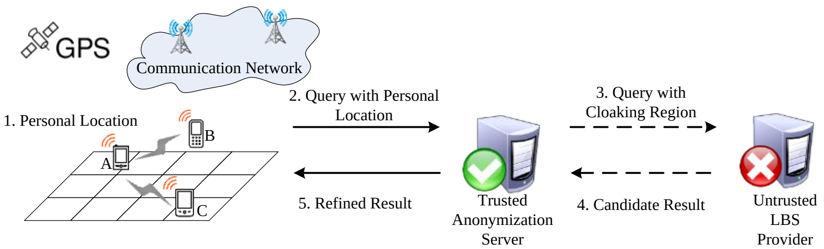
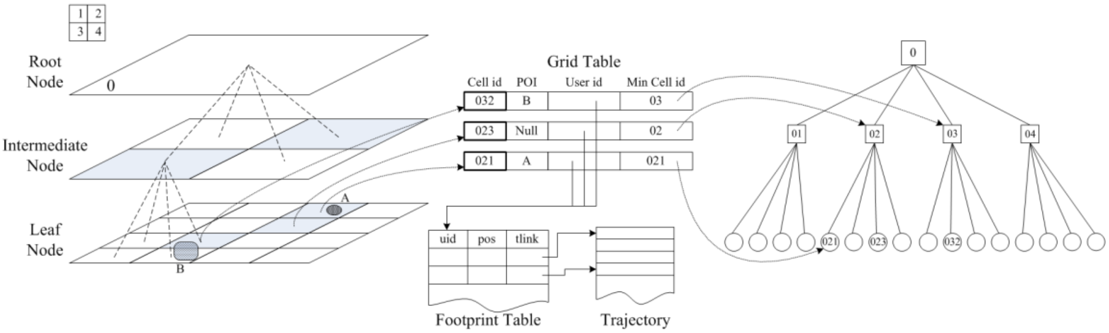


Figure 1. Anonymization System Architecture

4. Spatial Cloaking

In this section, we describe our cloaking method in two phases: *single-user cloaking* phase and *multi-user cloaking* phase. During single-user cloaking phase, each user is expected to initialize his cloaking region with the consideration of semantic location around. To illustrate this, we first define our quad-tree based method for cloaking.

As it is shown in Figure x 2, an area is recursively partitioned into a quad-tree with 3 levels. Most used quad-tree based cloaking method [14] has obvious weakness in semantic interest place representation. For example, there are two semantic places A and B that are shown as dark area in leaf nodes. A is fully contained in grid 021, however B is contained in both grid 032 and 034. According to previous work, we must perform a traverse heading the root node until the privacy semantic places is fully covered. This process can be time consuming and need many I/O times when there is a large quad-tree. In order to reduce time for querying grid, we proposed to build a table including the min grid information during the quad-tree initialization. Then, each grid is mapped with a node in quad-tree, which helps us easily find out that the minimum grid containing A is 021 and the minimum grid for B is 03 or {032, 034} according to user's privacy profile. Obviously, 03 is not the smallest cloaking as we expected, however this is generally accepted in existing work. With the implementation of a grid table, we can easily figure out the minimum grid of each POI, which can be nodes combination at same level (nodes {032,034} as a min grid of B). Also, we have a user id link from grid table to footprint table, which make it easy to figure out all the users exist in that grid.



Cell id	POI	User id	Min Cell id
032	B		03
023	Null		02
021	A		021

Figure 2. Grid based Cloaking Region Scheme

Then, we give our first algorithm for single-user cloaking region initialization.

4.1. Single-User Cloaking Phase

While most existing work focuses on how to minimize the sizes of cloaking region, we notice that there is an outstanding feature that semantic locations generally have a Minimum Bounding Rectangle (MBR), which is the minimum cover of semantic interest places. We aim to find the MBR to cover all semantic interest places that satisfy the privacy requirements. As exhibited in Figure 3, the whole area is divided into grid {N1~N9, M1~M6} (X~Y denotes labeled grid from X to Y). User's precise location is exhibited as a triangle *Q* and we have a certain privacy profile *r*. According to existing quad-tree cloaking method, we can identify the cloaking region as a set of dark grids {M1~M5, N2~N7} and {M6, N3~N6}. We proposed to consider semantic interest places that is {A, B, C} totally cover with the privacy requirements. Then, a MBR of {A, B, C} could be easily calculated as CR_1, which identify the cloaking region as a smaller set {M1~M4, N2~N6}. It is obvious that we achieve a smaller cloaking region, which is an important criterion for choosing a cloaking region. More important feature is that we obtain a cloaking region against *center-of-cloaked-area attack*. As it is shown in Figure 3, *Q* is the original query issuer, while *Q'* is the center of cloaked region CR_1. We can further improve our method in multi-user cloaking phase against such kind of attack in next section.

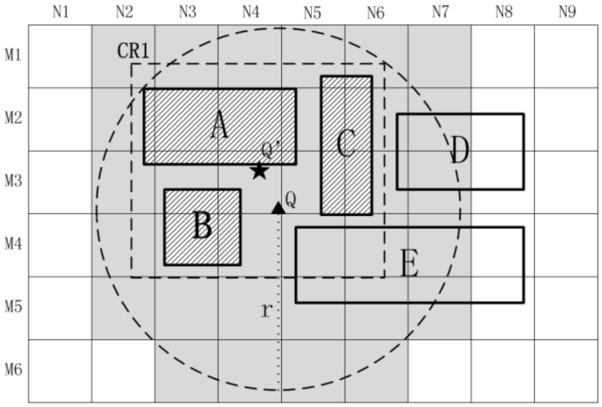


Figure 3. Example of MBR-based Cloaking Region

According to our method, each user initialized his cloaking region with a personal privacy profile. Then, we should consider another privacy metric *k-anonymity,* which means *k* users should be blurred in the cloaking region.

4.2. Multi-User Cloaking Phase

The basic idea of P2P *k-anonymity* spatial cloaking algorithm is that a mobile user communicates with other peers via multi-hop routing to find at least *k-1* peers, which make the query issuer indistinguishable among *k* users within the cloaked region. Users in P2P environment are assumed to be safety in existing approaches [15, 25], however this is not true in real environment. An adversary can disguise to be a normal user and obtain others' privacy information easily. However, there is a serious update problem while user movement always happens around edge of cloaking region, known as *user frequent update* problem. Figure 4 exhibits an example of multi-user cloaking procedure against these two problems by illustrating *multi-user sharing cloaking* and *representative cloaking region*.

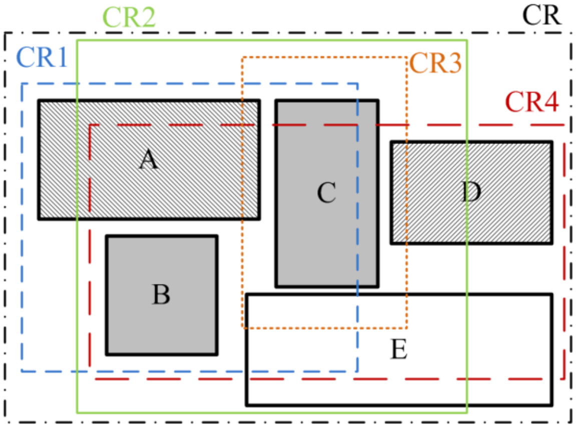


Figure 4. Cloaking Region from Multi-users

Each user is first cloaked with in *single-user cloaking* phase with semantic locations (POIs) and given a link to *k* nodes containing corresponding POIs. For example, let U_4 be a query issuer with its initial cloaking region CR_4. Here, we assume that users can also be an adversary, which means CR_4 may be disclose his location information if he share location information with neighbors. We start the searching step with cloaking region CR_4 instead of exact location of U_4.

1. Initial Step :
   a) Notice that there are two semantic locations {***B***, ***D***} fully included in $\boldsymbol{CR_4}$, then we search with grid table proposed in Fig. 3 to find all the other cloaking region containing {***B***} or {***D***}.
   b) As $\boldsymbol{CR_1}$ contains {***A***, $\underline{\boldsymbol{B}}$, ***C***}, $\boldsymbol{CR_2}$ contains {$\underline{\boldsymbol{B}}$, ***C***}, we should add $\boldsymbol{CR_1}$ and $\boldsymbol{CR_2}$ to our candidate cloaking sets.
2. Expand Step :
   Considering current cloaking sets {$\boldsymbol{CR_4}$, $\boldsymbol{CR_1}$, $\boldsymbol{CR_2}$}, we perform expanding with new added semantic location {***C***}. Then $\boldsymbol{CR_3}$ is found and need to be added to candidate cloaking region sets.

Algorithm stops when there is *k* users found in candidate cloaking region sets and combine them into CR. **Algorithm 1** depicts the pseudo code of our multi-user cloaking algorithm.

Algorithm 2. Generating Multi-User Cloaking Region

```
INPUT :   User initial cloaking region $CR_q$ , POIs list $P\{P_1, \dots , P_n\}$ ,
          Grid Map $gMap[M \times N]$ , privacy profile $k$ users
OUTPUT :  Cloaking Region $CR$, Represenive Cloaking Region $RCR$,
          Tolerant Time for Update $T_{tol}$ , Edge User List $UList$
POIList $\leftarrow \{ \emptyset \}$
initial $CR$ with $CR_q$;
POIList $\leftarrow$ POIs $P$ contained in $CR_q$;
while number of users in $CR < k$
    for each POI $P_i$ in $CR$
        broadcast to $CR_i$ which contains $P_i$;
        // $CR_i$ can be found easily with grid table
        count $P_i$;
        add each $P_j$ in $CR_i$ to POIList;
    end for
    $CR = CR_i + CR$;
end while
compute $CR$ with grid map $gMap[M \times N]$;
compute $RCR$ with grid map $gMap[M \times N]$;
get all POI $P_j$ in $RCR$;
$P_k$ = POIList – $P_j$;
// get all POIs not in $RCR$
$T_{tol}$ = minimum { width of $P_k$'s min grid / max speed of $P_k$;}
$UList$ = users not in $RCR$;
output $CR$ with grids;
output $RCR$ with grids;
```

With the further consideration, semantic location {B} and {C} have top frequency of appearance. Then we define them with corresponding grids as core region. We give the formal definition in the following. According to the experimental evaluation in Section 5, core region helps a lot in reducing communication cost against user movement.

Definition 1. [**Core Region]** Core region is defined as a set of semantic locations with highest frequency of appearance in a cloaking region *CR*. The corresponding grid nodes of core region are defined as a representative cloaking region (*RCR*).

Definition 2. [**Edge Region]** Edge region is defined as a set of semantic locations exist in the cloaking region but not in the core region.

5. Experimental Evaluation

5.1. Experimental Environment

We conduct experiment on a desktop PC with AMD Phenon II X4 945 Processor 3.00 GHz and 4GB main memory. We modified the well-known Thomas Brinkhoff Network-based Generator of Moving Objects [17] to generate moving object for privacy preservation evaluation. We implement several existing cloaking algorithm as baseline and perform spatial cloaking on the road map of Oldenberg, Germany. Parameters setting are given in Table 2.

We evaluate the performance of our algorithm with respect to some important performance measures. (1) Cloaking region size, which gives the average size of cloaking region. (2) Anonymization success rate, which indicates scalability of spatial cloaking algorithm. (3) Center-of-cloaked-area distribution, which indicates the privacy attack probability in a cloaking region. (4) Ratio of cloaking region variation, which indicates the stability of spatial cloaking algorithm towards user movement.

Table 2. Default Parameters in Modified Brinkhoff Generator

Parameter Name	Parameter Value
Number of Users	10,000~100,000
Speed of Users	20~80 km/hour
k-anonymity	5-30
l-diversity	3-10
Number of POIs	100,000
Min Grid Size(width)	20~120 meter
Semantic Locations	8000

5.2. Performance Evaluations

- **Impact of Center-of-Area Attack**

As we have discussed, only [23] support prevention of center-of-area attack in previous research. So we compare it with our proposed method SCMC. It is obvious that both P2P-CA and our method can output a probability close to 1/k to guess query issuer. To evaluate how much query issuer's location deviate the center of cloaking region. We generate a small rectangle CR' in each cloaking region CR, which has the same center point with CR but only has a half of CR's width. The experiments are conducted in 20 times. As it is shown in Figure 5, the distribution value stands for how much an adjusted location Q' is deviated from the center Q. The distribution value is 0 when Q' shows at Q, while it stands for 100 when Q' shows on the edge of CR. We can see that P2P-CA successfully adjust query issuer location away from cloaking center, however, most of them drop outside of CR' with the observation that output most distribution value over 50. Our proposed SCMC renders well-distributed value during the test, which means more effective against center-of-area attack.

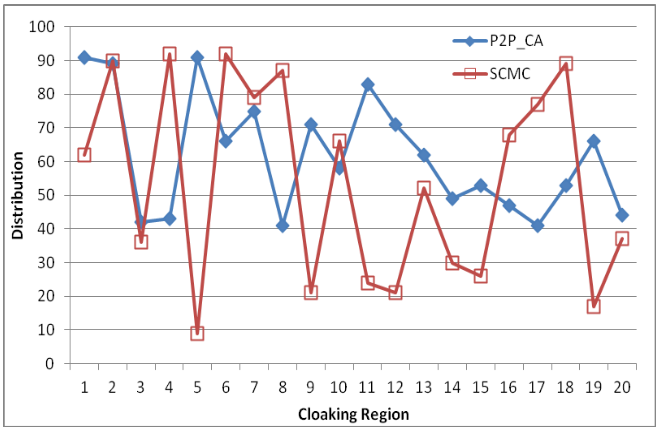


Figure 5. Distribution of Query Issuer

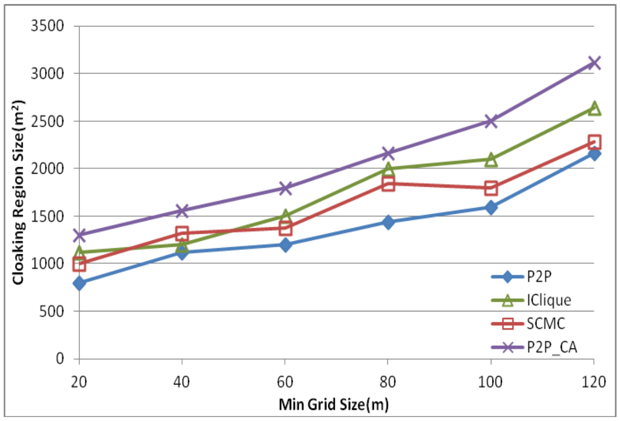


Figure 6. Cloaking Size over Grid Size Variation

- **Impact of Grid Size**

We propose evaluate the impact of different grid map size towards cloaking. It is easy to understand that P2P-CA show the largest cloaking size because there is a cloaking adjust scheme. Our method SCMC render a good performance due to the MBR adopted in semantic cloaking. The original P2P method output the smallest cloaking size as a result of that no semantic location are consider in the cloaking. Finally, all these four method show an increasing of cloaking size while grid size increased as it is shown in Figure 6.

- **Impact of Anti-Similar Location Attack**

Similar location attack is seldom studied in previous research, hence, we propose to compare with the only work SemGraph and a general P2P algorithm. We generate users range from 10k to 100k including 20% users as query issuers. We calculate the ratio of similar location in each cloaking region and output the performance in Figure 8. It is obvious that we achieve a better performance against similar location attack compared with SemGraph. This experiment proves that our weight update scheme is effective.

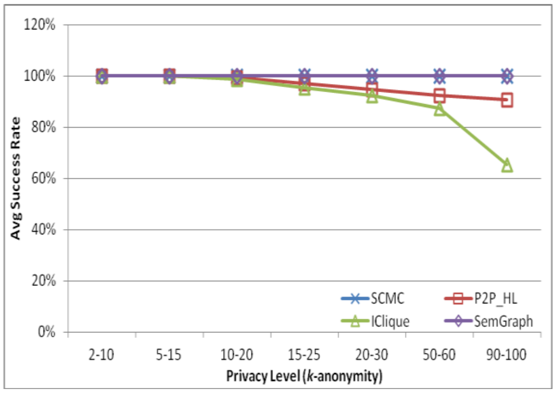
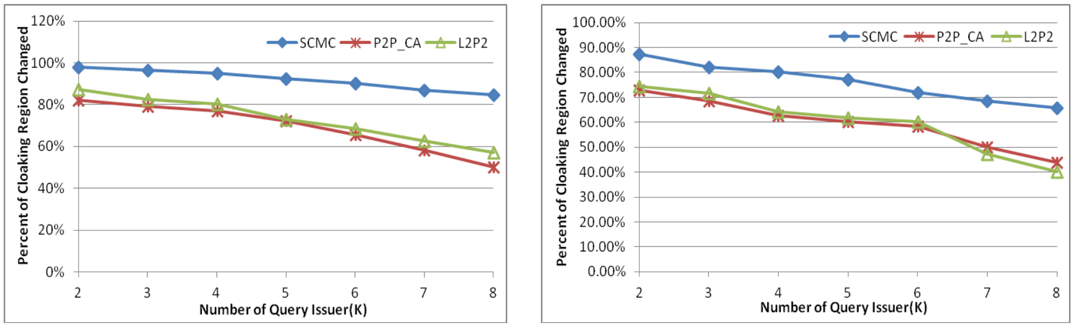


Figure 7. Analysis of Similar Location Attack

- **Impact of Movement**

Continuous movement of query issuer may involve a communication overhead and high computation cost of cloaking. In this experiment, we investigate the stability of our method over various user movement speeds. As it is shown in Figure 9, we define the percent as how much a CRq change to CRq' while q moves. We conduct our experiment with two conditions : Figure 9 (a) show the result of CRq has overlap with representative cloaking region (RCR) which indicates that q is probability located in RCR, while (b) exhibits the result of CRq have no overlap with RCR. The ratio of our proposed method sinks while other method suffers more when query issuers increased. It is obvious that movement in RCR do not affect as much as that outside RCR, which indicates that RCR domain the whole cloaking region.



(a) (b)

Figure 9. Different Moving Speed; (a) Query Issuer's CR Overlap with RCR (b) Query Issuer's CR non-overlap with RCR

6. Conclusion

A lot of attentions have been drawn on location privacy protection in location-based services and trajectory data publication from the viewpoint of industry and academia. While most existing work focuses on how to minimize the sizes of cloaking regions, the relation between cloaking regions and semantic locations is unclear. We proposed a two phase method, single-user cloaking and multi-user cloaking, to select cloaking region with the consideration of semantic locations. The proposed algorithm can be properly implemented in both centralized and P2P system, and it renders a good performance against various attacks from service providers and users. Our experimental results on synthetic dataset demonstrate that our proposed method is reasonable, accurate, effective and efficient for location privacy protection.

Acknowledgements

This work was financially supported by the Natural Science Foundation of China (41201378), Natural Science Foundation Project of Chongqing CSTC (cstc2012jjA40014), Young Scientist Foundation of Chongqing University of Posts and Telecommunications (A2013-36), Talent Foundation of Chongqing University of Posts and Telecommunications (A2014-06), and Creative Foundation of WenFeng (A2014-12).

References

[1] L. Wang and X. F. Meng, "Location Privacy Preservation in Big Data Era: A Survey", Ruan Jian Xue Bao/Journal of Software, vol. 25, no. 4, **(2014)** (in Chinese).

[2] X. Zhang, Y. Xia and H. Y. Bae, "A Semantic Cloaking Method for Location Privacy Preservation", The 4th International Conference on Convergence and its Application, **(2014)** November 12-14; Jeju, South Korea.

[3] X. Zhang, G. B. Kim and H. Y. Bae, "An Adaptive Spatial Cloaking Method for Privacy Protection in Location-based Service", International Conference on ICT Convergence, **(2014)** October 22-24; Busan, South Korea.

[4] K. G. Shin, X. E. Ju, Z. G. Chen and X. Hu, "Privacy Protection for Users of Location-Based Services", IEEE Wireless Communication, vol. 19, no. 1, **(2012).**

[5] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking", in Proc. of MobiSys, **(2003)** May 5-8; San Francisco, CA, USA.

[6] T. Xu and Y. Cai, "Feeling-Based Location Privacy Protection for Location-Based Services", The 16th ACM Conference on Computer and Communication Security, **(2009)** November 9-13; Chicago, IL, USA.

[7] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location-based Services", IEEE Proc. Int'l. Conf. Pervasive Services, **(2005)** July 11-14.

[8] Z. Chen, "Energy-Efficient Information Collection and Dissemination in Wireless Sensor Networks", Ph.D. Thesis, University of Michigan, **(2009).**

[9] B. Hoh and M. Gruteser, "Protecting Location Privacy through Path Confusion", IEEE SecureComm, **(2005).**

[10] B. Y. Lee, J. O. Oh, H. J. Yu, and J. Kim, "Protecting Location Privacy Using Location Semantics", KDD, **(2011)** August 21-24; San Diego, USA.

[11] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The New Casper: Query procesing for location services without compromising privacy", in Proc. of VLDB, **(2006).**

[12] H. Hu and J. Xu, "Non-Exposure Location Anonymity", IEEE ICDE, **(2009)**March 29-April 2; Shang Hai, China.

[13] G. Ghinita, "Private Queries in Location Based Services: Anonymizers Are Not Necessary", ACM SIGMOD International Conference on Management of Data, **(2008)** June 9-12; Vancouver, Canada.

[14] H. I. Kim, Y. S. Shin, and J. W. Chang, "A Grid-based Cloaking Scheme for Continuous Queries in Distributed Systems", **(2011)** August 31-September 2; Pafos.

[15] C. Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer Spatial Cloaking Algorithm for anonymous Location-based Service", In: Proceedings of the ACM Symposium on Advances in Geographic Information Systems, GIS, **(2006).**

[16] X. Pan, J. L. Xu, and X. F. Meng, "Protecting Location Privacy against Location-Dependent Attacks in Mobile Services", IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 8, **(2012).**

[17] T. Brinkhoff, "Network-Based Generator of Moving Objects", http://www.fh-oow.de/institute/iapg/personen/brinkhoff/generator/, **(2008).**

[18] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid", Proc. Int'l Conf. World Wide Web, **(2008)** April 21-25; Bei Jing, China.

[19] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, "Anonymity in Location-Based Services: Towards a General Framework", Proc. Int'l Conf. Mobile Data Management (MDM), **(2007).**

[20] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms", IEEE TMC, vol. 7, no. 1, **(2008).**

[21] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems", The 16th International World Wide Web Conference, **(2007)** May 8-12; Banff, Alberta, Canada.

[22] G. Ghinita1, P. Kalnis, and S. Skiadopoulos, "MobiHide: A mobile peer-to-peer system for anonymous location-based queries", Advances in Spatial and Temporal Databases, **(2007).**

[23] C. Y. Chow, M. F. Mokbel and X. Liu, "Spatial Cloaking for Anonymous Location-based Services in Mobile Peer-to-Peer Environments", **(2012).**

[24] J. Meyerowitz and R. R. Choudhury, "Hiding Stars with Fireworks: Location Privacy Through Camouflage", MobiCom, ACM, **(2009).**

[25] M. F. Mokbel and C. Y. Chow, "Challenges in preserving location privacy in peer-to-peer environments", Web-Age Information Management Workshops, **(2006)** June; Hong Kong, China.

[26] K. P. N. Puttaswamy, S. Y. Wang, T. Steinbauer and D. Agrawal, "Preserving Location Privacy in Geosocial Applications", IEEE Transactions on Mobile Computing, vol. 13, no. 1, **(2013).**

Authors

Xu Zhang, he is an assistant professor of Chongqing University of Posts and Telecommunications, received Ph.D degree from Inha University, South Korea. His research area mainly includes ubiquitous computing (sensor network, localization), location-based service, large scale data processing, database, etc..

Email: zhangx@cqupt.edu.cn

Ying Xia, she received the Ph.D. degree in computer science and technology from the Southwest Jiaotong University, China. Currently, she is a professor at Chongqing University of Posts and Telecommunications, China. Her research interests include location-based service, spatial database and cross-media retrieval.

Email: xiaying@cqupt.edu.cn

HaeYoung Bae, he is tenured full professor of Inha University of Korea, and he is honorary professor of the Chongqing University of Posts and Telecommunications of China. His research area mainly includes database and spatial information processing.

E-mail: hybae@inha.ac.kr