Journal of The Korea Society of Computer and Information
Vol. 18, No. 3, March 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.3.047

이동 객체 정보 보호를 위한 그리드 기반 시멘틱 클로킹 기법

장 욱*, 신숭선*, 김경배**, 배해영*

Grid-based Semantic Cloaking Method for Continuous Moving Object Anonymization

Xu Zhang*, Soong-Sun Shin*, Gyoung-Bae Kim**, Hae-Young Bae*

요 약

최근 스마트폰의 발전에 따라서 많은 위치 기반 서비스가 활용되고 있으며, 위치 정보 노출로 인한 문제점이 사회적 이슈로 대두되고 있다. 기존의 잘 알려진 위치 정보 보호를 위한 공간 클로킹 기법은 사용자가 요청한 지역에서 위치 정보를 흐릿하게 처리하였다. 하지만 계속적으로 움직이는 이동 객체의 모든 지역을 클로킹하기에는 범위 공간이 무수히 넓어지는 문제를 가진다. 따라서, 본 논문에서는 이동 객체 정보 보호를 위한 그리드 기반 시멘틱 클로킹 기법을 제안한다. 제안 기법은 시멘틱 클로킹을 위하여 EMD 갱신 스키마를 확장하고 이동 객체를 위한 대표 보호지역의 클로킹을 정의하였다. 성능 평가에서는 제안 기법이 기존 기법에 비해 처리 시간과 공간 범위에서 안전성과 효율성을 높였다. 이를 통해, 성공적으로 다양한 적으로부터 지속적으로 움직이는 객체의 위치 개인 정보를 보호하여 기존의 방법을 능가하는 성능을 보인다.

▸ Keywords : 개인 위치 보호, 이동 객체, 시멘틱 클로킹, 위치기반 서비스

Abstract

Location privacy has been a serious concern for mobile users who use location-based services to acquire geographical location continuously. Spatial cloaking technique is a well-known privacy preserving method, which blurs an exact user location into a cloaked area to meet privacy requirements. However, cloaking for continuous moving object suffers from cloaked area size problem as it is unlikely for all objects travel in the same direction. In this paper, we propose a grid-based privacy preservation method with an improved Earth Mover's Distance(EMD) metric weight update scheme for semantic cloaking. We also define a representative cloaking area which

• This work was surported by INHA University.
• 제1저자 : 장 욱 • 교신저자 : 김경배
• 투고일 : 2013. 1. 30, 심사일 : 2013. 3. 5, 게재확정일 : 2013. 3. 11.
* 인하대학교 컴퓨터정보공학과(Dept. of Computer and Information Engineering, Inha University)
** 서원대학교 컴퓨터교육과(Dept. of Computer Education, Seown University)

protects continuous location privacy for moving users. Experimental implementation and evaluation exhibit that our proposed method renders good efficiency and scalability in cloaking processing time and area size control. We also show that our proposed method outperforms the existing method by successfully protects location privacy of continuous moving objects against various adversaries.

▸ Keywords : Location Privacy, Continuous Moving Object Anonymization, Semantic Cloaking, Location Based Service

I. 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 brings a considerable attention in privacy protection. How to protect users' privacy against potentially compromised LBS providers and attackers are of vital importance to existing systems. In general, existing work can be categorized into snapshot and continuous LBS. The mobile user only needs to report his current location to LBS provider once to request some service, while others have to report their location in a periodic manner to obtain certain continuous services. Privacy protection in continuous LBS and trajectory data publication has increasingly drawn attention from the research community and industry [1][22][23].

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 [2-4]. 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 [3].

A straightforward and generally adopted method in privacy protection is spatial cloaking, which proposed to blur a user's exact location into a cloaked area that satisfies the user specified privacy requirements [5-8]. Most researches consider privacy preservation problem without considering continuous location update, which have serious problem on supporting continuous queries. First, the

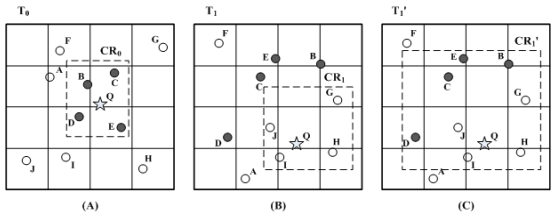

Fig. 1. Location protection in snapshot & continuous LBS

cloaking area is well initialized as a minimum area, however it will become larger due to user's movement. As it is shown in Fig. 1(A), Q is the query issuer in snapshot LBS with a privacy profile k=5, then it is easy to calculate the cloaking area region CR0{B, C, D, E, Q} at time T0. Then user Q issue another query with its updated location and obtain a new cloaking area region CR1{I, J, G, H, Q} at time T1. It is easy for an adversary to detect user Q with a comparison between CR0 and CR1. A straightforward method to prevent this attack is to keep all the users in the cloaking area. However, this method may generate a large sized cloaking area as it is shown in Fig. 1(C). CR1′ is the generated cloaking area in continuous LBS with the consideration of containing all initial members.

Second, mobile users may issue query frequently

which will cause a high communication overhead and great time consumption for cloaking area generation. Due to the communication cost is expensive for mobile user, it is intuitive to share information between users instead of frequently request from service provider. The main idea of peer-to-peer (P2P) spatial cloaking algorithm is that when a mobile user wants to obtain services from a LBS provider, he can collaborates with other peers via multi-hop communication to blur his location into a cloaked area [6]. There is a critical limitation that only service providers are considered as adversary while users are regarded safety in previous cloaking methods. Intuitively, both service providers and user could be a potential threat to users who want to use location based service in real environment.

Third, query issuer is easy to be inferred at the center of cloaking area, which is introduced as "center-of- cloaked-area" attack and well studied with cloaking re-adjusting method in [6]. Another research in [9] proposed a two step cloaking generation method against this attack. Expand step is used to enlarge the cloaking area toward four directions to cover at least k′ users (k′>k). Reduce step is done by deleting some rows or columns for each direction to obtain a minimum area as the initial cloaking area.

Privacy in continuous LBS is more challenging than snapshot LBS because adversaries could use the spatial and temporal correlations in the user's location samples to infer location information[1]. In this paper, we propose a novel method to provide efficient location privacy preservation in continuous LBS with the consideration of location semantics. Our proposed method has two phase : (I) single-user cloaking and (II) multi-user cloaking. Query issuers initialize his cloaking area with the consideration of semantic locations nearby and maintain the continuous location update with a modified Earth Mover's Distance (EMD) graph in phase I. Cloaking area expands with overlapping semantic locations and reverse obtain users inside. Then, user send his initial cloaking area to neighbors and start to search peers around with overlapping semantic locations and process the multi-user cloaking phase to protect trajectory privacy. We conduct a series of experiments to evaluate the performance of our proposed algorithm with several existing works. Experimental results exhibit that our proposed method is efficient with continuous location update in terms of various metrics including cloaking area size, cloaking time, 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 II, we review the previous work in location privacy preservation. System architecture is introduced in Section III and then the grid-based semantic cloaking algorithm for continuous LBS is described in detail in Section IV. Finally we show our analysis and experimental results in Section V and draw a conclusion in Section VI.

II. Related Works

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 technique is the most popular privacy preservation method that supports many environments setting including centralized, distributed, peer-to-peer and wireless sensor networks, it also renders good performance in snapshot queries, continuous queries and trajectories [6]. 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 spatial cloaking techniques can be categorized into centralized [4][10-12], distributed [13-14], and peer-to-peer approach [6].

Casper [10] 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. CliqueCloak [21] provides a personalized k-anonymity model in which users can adjust their privacy level of anonymity to obtain a cloaking area. To our best of knowledge, SemGraph [5] is the first research, which deals with semantic cloaking with a graph based on Earth Mover's Distance (EMD). However, none of the above work considers semantic location and thus cannot avoid similarity location attack.

Snapshot spatial cloaking technique process each user location independently thus cannot ensure privacy for user trajectory and continuous query [20-21]. Spatial cloaking techniques over trajectory can be categorized into three kinds: group-based [15], distortion-based [16] and prediction-based [12], where the first two are proposed for real-time trajectories while the last one is for historical trajectories. Recent work GCCA (Grid-based Continuous Cloaking Area) [9] propose to generate cloaking area with expand-reduce phase and obtain an improved performance over Advance KAA (K-Anonymity Area) method [17]. However, it suffers from reduction strategy and expand-reduce involved with much more processing time. As it is shown in Fig. 2, GCCA algorithm first initial an expanded cloaking area in (A), and continue with reduction for each direction. However, there could be more than one candidate cloaking area as (B) and (C), which can not be distinguished from each other in GCCA.

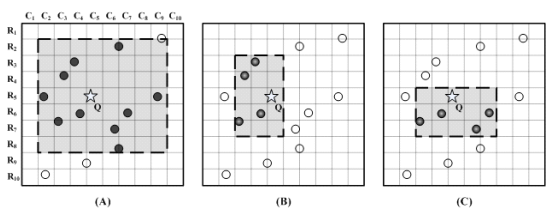

Fig. 2 Expand-Reduce cloaking candidate problem

In this paper, we propose to obtain the best cloaking area from all candidates and reduce processing time in continuous LBS location privacy protection. We describe our algorithm based on the following system framework in Section III.

III. System framework

We design our system architecture with a trusted anonymization server between location based service providers and mobile users in Fig. 3. 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. We propose to share initial cloaking area between users, which is generated in the single-user cloaking phase. For example, user A can obtain its cloaking area from user B and C's

Fig. 3. System Architecture

cloaking area and POIs while avoiding communication cost to anonymization server. This helps us to share information between users while avoiding leak important location information to adversary users.

The objective of an adversary is to compromise the user's location and infer sensitive information from them. In our threat model, we give the following assumptions:

1. We refer to both a malicious server and a malicious user as adversaries.

2. An adversary has the attack ability of center-of- cloaked-area, which means it can guess the query issuer by calculate the center of cloaking area.

3. An adversary is aware of some independent

location information and try to infer the whole trajectory information.

We describe our algorithm in the next section and discuss how to prevent these assumptions in continuous LBS.

IV. Continuous Cloaking Algorithm

Original k-anonymity model induces additional delay or large area, which are not suitable for continuous query and frequent location update. 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 area with the consideration of semantic locations around. To illustrate this, we first define our quad-tree based method for cloaking.

As it is shown in Fig. 4, an area is recursively partitioned into a quad-tree with 3 levels. Most used quad-tree based cloaking method [13] 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. 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 cloaking, 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. Also, we have a user id link from grid table to footprint table [15], which make it easy to figure out all the users exist in that grid.

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

4.1 Single-User Cloaking Phase

While most existing work focuses on how to minimize the sizes of cloaking area, 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. Then we propose to expand cloaking area by overlapping POIs and search with grid table in Fig. 4. As it is exhibited in Fig. 5, it is obvious that we achieve a smaller semantic cloaking area based on MBR of POIs A, B, C. More important feature is that we obtain a cloaking area against "center-of-cloaked-area" attack. Q is the original query issuer, while Q' is the center of cloaked area region CR1.

Then, we consider that a user privacy profile r with l-diversity metric, which means at least l POIs must be included in the cloaking area. We modified the location semantic graph proposed in [5] for l-diversity cloaking. A distance between semantic locations to user location is computed with Earth Mover's Distance (EMD)[4], which is proposed originally based on the minimal amount of work needed to transform one distribution into another by

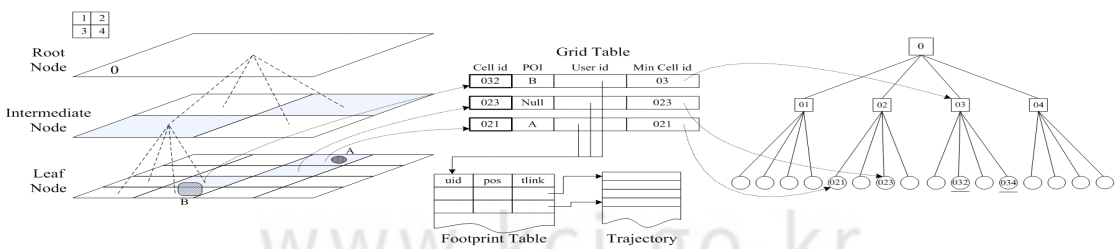

Fig. 4. Grid-based Cloaking Scheme

moving distribution mass between each other.

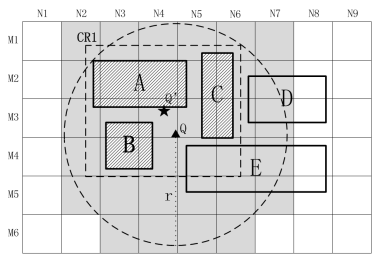

Fig. 5. MBR-based Cloaking

We illustrate the location semantic graph in Fig. 6 by keeping the same definition in [5]. A prior belief is considered as the adversary do not know the cloaking area, which means an adversary's knowledge is the location semantics of an entire area since he has no idea where a mobile user is located. A posterior belief is considered as the adversary has already known the cloaking area, which means he can obtains more specific location semantics corresponding to the cloaking area. As it is shown in Fig. 6, the node represents semantic locations and the edge weight represents EMD between corresponding nodes. The prior belief is represented as a location semantic graph in Fig. 6 (b), while the posterior belief is a more elaborated graph upon prior belief shown as Fig. 6 (c) and (d).

Note that the triangle Q' is the query issuer with 4 semantic places {P1, P2, P3, P4} with an assumption that P1 and P2 are considered with education semantic property, while P3 and P4 are medical related. Now, the issuer Q' has two choice to initial his own cloaking area region represented as CR1{P1, P2} or CR2{P1, P3}. Then we are going to evaluate the safety of each cloaking area.

It is easy to understand that in Fig. 5 (b), each semantic place has an average probability 0.25. According to [5], a node in location semantic graph is converted into a discrete domain in EMD, and an edge weight is converted into a ground distance dij. Then, the numerical computational results of CR1 and CR2 are :

$$D_{EMD}(P_{CR_1}, P_E) = \min_f \sum_i \sum_j f_{ij} d_{ij} = f'_{13} d_{13} + f'_{14} d_{14} + f'_{23} d_{23} + f'_{24} d_{24}$$
$$= 0.25 \times 0.4 + 0 \times 0.7 + 0 \times 0.6 + 0.25 \times 0.5 = 0.225 \quad (1)$$

$$D_{EMD}(P_{CR_2}, P_E) = \min_f \sum_i \sum_j f_{ij} d_{ij} = f'_{12} d_{12} + f'_{14} + f'_{32} d_{32} + f'_{34} d_{34}$$
$$= 0.25 \times 0.4 + 0 \times 0.7 + 0 \times 0.6 + 0.25 \times 0.6 = 0.25 \quad (2)$$

Where PCRk indicates the posterior belief of cloaking area region CRk, PE indicates the prior belief. CR1 is considered more secure than CR2 based on DEMD(PCR1, PE) 〈 DEMD(PCR2, PE). However, this method cannot solve location similarity attack, where the adversary can guess that the user can be a student or teacher who always stays around education related POIs. To solve this problem, we proposed to update weight between similar POIs in location semantic graph. The EMD between similar POIs should be reduced which means there is no semantic difference between them. As it is shown in Fig.6 (c) and (d), weight between P1 and P2 is reduced to 0. Then we perform numerical computation again:

$$D_{EMD}(P_{CR_1}, P_E) = \min_f \sum_i \sum_j f_{ij} d_{ij}$$
$$= 0.25 \times 0.4 + 0 \times 0.7 + 0 \times 0.6 + 0.25 \times 0.5 = 0.225 \quad (3)$$

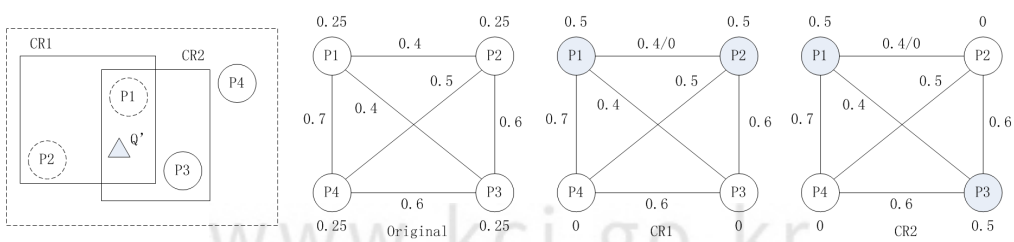

Fig. 6. Location semantic graph to generate initial cloaking area

$$D_{EMD}(P_{CR_i}, P_E) = \min_f \sum_i \sum_j f_{ij} d_{ij}$$
$$= 0.25 \times 0 + 0 \times 0.7 + 0 \times 0.6 + 0.25 \times 0.6 = 0.15 \quad (4)$$

Which means CR2 is more secure and should be considered as an initial cloaking area of Q'. The proposed is obvious to obtain the best cloaking area against the problem in Fig. 2 and it is shown to reduce cloaking processing time in performance evaluation in Section V. Then, we propose to involve multi-user movement to protect trajectory privacy, however, the existing SemGraph did not show its efficiency in continuous LBS.

4.2 Multi-User Cloaking Phase

A trajectory contains all information of a continuous moving object. In this section, we propose to protect the continuous moving object privacy by trajectory anonymization. In our assumption in Section III, we do not want to disclose the whole trajectory information when some independent location has been exposed to adversary. However, publishing original trajectory may cause critical breaches of privacy. We introduce a multi-user cloaking method to maintain the cloaking area size at a constant level and protect whole trajectory privacy. As it is shown in Fig. 7, we have 4 initial cloaking area regions {CR1, CR2, CR3, CR4} from 4 users {U1, U2, U3, U4} around. There are 6 trajectories shown with 3 timestamps T1, T2 and T3. If an adversary can identify the trajectory as the target user, the adversary can obtain extra knowledge to add to the prior knowledge [19]. We propose to generate multi-user cloaking among trajectories at time T2, which means 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 U4 be a query issuer with its initial cloaking area region CR4. Here, we assume that users can also be an adversary, which means CR4 may be disclose his location information if he share location information with neighbors. We start the peer-to-peer searching step with cloaking area region CR4 instead of exact location of U4.

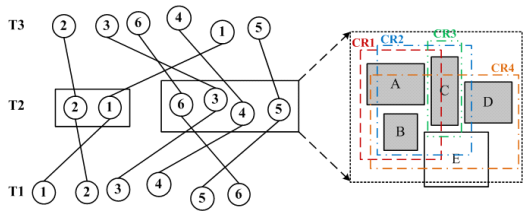

Fig. 7. Trajectory anonymity

1. Initial Step :

a) Notice that there are two semantic locations {B, D} fully included in CR4, then we search with grid table proposed in Fig. 3 to find all the other cloaking area containing {B} or {D}.

b) As CR1 contains {A, B}, CR2 contains {B, C}, we should add CR1 and CR2 to our candidate cloaking sets.

2. Expand Step :

Considering current cloaking sets {CR4, CR1, CR2}, we perform expanding with new added semantic location {C}. Then CR3 is found and need to be added to candidate cloaking area sets.

Algorithm stops when there is k users found in candidate cloaking area sets and combine them into CR, with the consideration of both l-diversity metric in single-user phase and k-anonymity metric in multi-user phase.

With the further consideration, semantic location {B} and {C} have top frequency of appearance. Then we define them with corresponding grids as core area. We give the formal definition in the following.

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

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

Semantic locations in a representative cloaking

area stand for a user dense area of the cloaking area region CR. We argue that semantic locations in RCR keep stable within a time duration. With the previous definitions, it is easy to understand that RCR dominate the cloaking area. In other word, if there is a query issuer q with its cloaking area region CR and RCR, when q moves for a short time, q may be obtain a new cloaking area however RCR remains. We maintain the RCR in trajectories when dealing with continuous moving object anonymization and discuss the efficiency in Section V.

V. Performance 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 [18] to generate moving object for privacy preservation evaluation and perform spatial cloaking on the road map of Oldenberg, a city of 15 * 15 km2 which contains 6105 nodes and 7035 edges. We implement Advanced KAA [17], GCCA [9] and a semantic cloaking method SegGraph [5] as baseline and denote our method as SCMC (Single Cloaking and Multiple Cloaking). All the semantic locations are randomly generated on the map. The parameters are given in Table 1.

Table 1. Parameters setting

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

As it is analyzed in section IV, our proposed method can protect "center-of-cloaked-area" attack well. We evaluate the performance of our algorithm with respect to the following performance measures. (1) Similar locations in a cloaking area, which indicates privacy level. (2) Cloaking area size, which indicates the communication overhead. (3) Cloaking processing time, which indicates the efficiency of the algorithm.

- Anti-Similar Location Attack

Semantic location attack is seldom studied in existing research, hence, we propose to compare with the only work SemGraph and a general continuous cloaking method GCCA. We generate users range from 10k to 100k including 20% users as query issuers. We calculate the ratio of similar location in each cloaking area and output the performance in Fig. 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 against similar location attack.

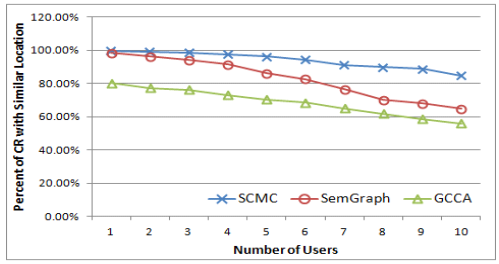

Fig. 8 Similar location in cloaking area

- Cloaking Processing Time

Cloaking processing time is an important criterion for continuous location protection method evaluation. It is shown in Fig. 9 that GCCA and our method exhibit better performance than KAA. This is because grid-based structure help a lot in reducing computational overhead. We achieve a little improvement in processing time over GCCA. This is

because GCCA need more time for grid expansion and reduction operation.

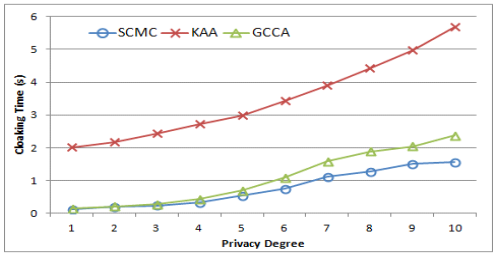

Fig. 9 Cloaking processing time

- Cloaking Area Size

Cloaking area size indicate communication overhead during privacy protection. It is expected to obtain a smaller cloaking area size with fewer candidates to reduce communication cost. We perform evaluation with 6 different privacy degrees of (k-anonymity, l-diversity). As the average size is shown in Fig. 10, it is obvious that GCCA and KAA can obtain a smaller size. However, our method obtain an improved performance when the privacy degree increase. This is because a high privacy degree always indicates more moving objects needed to be considered and query issuer can be away from center of cloaking area. It is obvious that more users are located in a dense area, which is near the semantic locations. Then our semantic cloaking method benefit from this and obtain the minimum cloaking area size based on MBR. We also implemented KAA and GCCA to consider semantic locations, which exhibit an increasing cloaking area size in the figure.

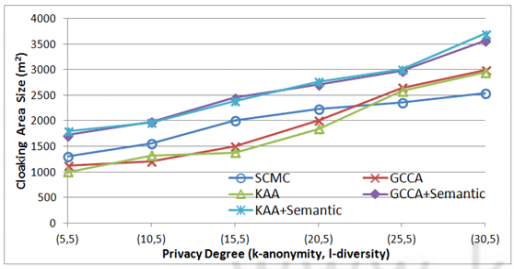

Fig. 10 Cloaking area size

VI. Conclusion

A lot of attentions have been drawn on privacy protection in location-based services and trajectory data publication from the viewpoint of industry and academia. In this paper, we proposed a two phase method, single-user cloaking and multi-user cloaking, to achieve trajectory anonymization in continuous LBS with the consideration of semantic locations. The proposed algorithm renders a good performance against various attacks from service providers and users. Our experimental results on synthetic dataset demonstrate that our proposed method is effective and efficient for continuous location privacy protection that can reduce communication overhead with a minimum cloaking area.

참고문헌

[1] C.Y. Chow, and M.F. Mokbel, "Trajectory Privacy in Location-based Services and Data Publication," ACM SIGKDD Explorations Newsletter, Vol. 13, No. 1, pp. 19-29, 2011.

[2] A. Pingley, W. Yu, N. Zhang, X.W. Fu, and W. Zhao, "Cap: A Context-Aware Privacy Protection System for Location-Based Services," IEEE ICDCS, pp. 49-57, June 2009.

[3] 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, pp. 30-39, February, 2012.

[4] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid," Proc. Int'l Conf. World Wide Web (WWW), pp. 237-246, 2008.

[5] B.Y. Lee, J.O. Oh, H.J. Yu, and J. Kim, "Protecting Location Privacy Using Location Semantics", Proc. Int'l. Conf. Knowledge

Discovery and Data Mining (KDD), pp. 1289-1297, 2011.

[6] C.Y. Chow, M.F. Mokbel, and X. Liu, "Spatial Cloaking for Anonymous Location-based Services in Mobile Peer-to-Peer Environments," Vol. 15, No. 2, pp. 351-380, 2012.

[7] H.I. Kim, Y.S. Shin, and J.W. Chang, "A Grid-based Cloaking Scheme for Continuous Queries in Distributed Systems," Proc. Int'l. Conf. Computer and Information Technology, pp. 75-82, 2011.

[8] 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, pp. 1506-1519, 2012.

[9] H.J. Lee, B.S. Oh, H.I. Kim, and J.W. Chang, "Grid-based Cloaking Area Creation Scheme Supporting Continuous Location-based Services," Proc. Int'l. Conf. Applied Computing, pp. 537-543, 2012.

[10] M.F. Mokbel, C.Y. Chow, and W.G. Aref, "The New Casper: Query procesing for location services without compromising privacy," Proc. Int'l. Conf. Very Large Databases (VLDB), pp. 763-774, 2006.

[11] B. Gedik, and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," IEEE Transactions on Mobile Computing , Vol. 7, No. 1, pp. 1-18, 2008.

[12] T. Xu, and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-based Services," Proc. Int'l. Conf. Computer Communications (INFOCOM), pp. 547-555, 2008.

[13] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems," Proc. Int'l. Conf. World Wide Web, pp. 371-380, 2007.

[14] G. Ghinita1, P. Kalnis, and S. Skiadopoulos, "MobiHide: A Mobile Peer-to-Peer System for Anonymous Location-based Queries," Proc. Int'l. Conf. Advances in Spatial and Temporal Databases, pp. 221-238, 2007.

[15] C. Chow, and M.F. Mokbel, "Enabling Private Continuous Queries for Revealed User Locations," Proc. Int'l. Conf. Advances in Spatial and Temporal Databases, pp. 258-273, 2007.

[16] X. Pan, X.F. Meng, and J. Xu, "Distortion-based Anonymity for Continuous Queries in Location-based Mobile Services," Proc. Int'l. Conf. ACM SIGSPATIAL on Advances in Geographic Information Systems, 2009.

[17] T. Xu, and Y. Cai, "Location Anonymity in Continuous Location-based Services," Proc. Int'l. Conf. on Advances in Geographic Information Systems, pp. 221-238, 2007.

[18] Thomas Brinkhoff Network-Based Generator of Moving Objects, http://www.fh-oow.de/institute/iapg/personen/brinkhoff/generator/, 2008.

[19] T. Takahashi, and S. Miyakawa, "CMOA: Continuous Moving Object Anonymization," Proc. Int'l. Conf. Database Engineering & Applications, pp. 81-90, 2012.

[20] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. Int'l. Conf. Management of Data (SIGMOD), pp. 121-132, 2008.

[21] Y.L. Wang, H. Zhou, Y.J. Wu, and L. Sun, "Preserving Location Privacy for Location-based Services with Continuous Queries on Road Network," Proc. Int'l. Conf. Computer Science & Education, pp. 822-827, 2012.

[22] T.G. Kim, S.S. Shin, W.I. Chung, and H.Y. Bae, "Effective Indexing of Moving Objects for Current Position Management in Road Networks," Journal of the Korea Society of Computer and Information, Vol. 16, No. 10, pp. 33-43, 2011.

[23] S.S. Shin, G.B. Kim, and H.Y. Bae,

"FingerPrint Building Method Using Splite-tree based on Indoor Environment," Journal of the Korea Society of Computer and Information, Vol. 17, No. 6, pp. 173-182, 2012.

저 자 소 개

Xu Zhang
2000~2004: Qingdao University, P.R. China(B.S).
2007~2010: Chongqing University of Posts and Telecommunications. P.R. China(M.S)
2010~present: Computer Science and Information Engineering, Inha University, Ph.D Candidate
Research Interest: Location Privacy, LBS, Cloud Computing
Email : zhangxu.jn@gmail.com

Soong-Sun Shin
2006: Computer Education, Seowon University
2008: Computer Science and Engineering, Inha University(M.S)
2013: Computer Science and Information Engineering Inha University(Ph.D)
Research Interest: Database, Spatial Database, LBS, u-GIS, DSMS
Email : hermit7999@gmail.com

Gyoung-Bae Kim
1992: Inha University 전자계산학과 학사.
1994: Inha University 전자계산공학과 석사.
2000: Inha University 전자계산공학과 공학박사
2000: 한국전자통신연구원 선임연구원
현 재: Seowon Univerisity 컴퓨터교육과 교수
관심분야: 데이터베이스, GIS, 클라우드컴퓨팅, 컴퓨터교육론
Email : gbkim@seowon.ac.kr

Hae-Young Bae
1974: Physical Engineering Depart. Inha Univ. (B.S)
1978: Computer Science and Engineering Depart. Yonsei Univ.(M.S)
1989: Computer Science and Engineering Depart. Soongsil Univ.(Ph.D)
1982~present: Computer Science and Information Engineering Depart. Inha University, Prof.
Research Interest: Database, patial Database
Email : hybae@inha.ac.kr