International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.133-146
http://dx.doi.org/10.14257/ijsia.2014.8.1.13

Sensitive Semantics-Aware Personality Cloaking on Road-Network Environment

Min Li[1, 2], Zhiguang Qin[1] and Cong Wang[1]

[1]*School of Computer Science & Engineering, University of Electronic and Technology of China, Chengdu, China*
[2]*College of Computer Science, Sichuan Normal University, Chengdu, China*
Email: lm_turnip@126.com, qinzg@uestc.edu.cn, wongcong@gmail.com

Abstract

*Recently, several cloaking methods based on **K**-anonymity and **L**-diversity has been proposed to protect the user's location privacy for Location-based Services (LBS). Considering that a cloaking region could contain some semantic places, which can easily endanger the user's privacy, it is not safe to cloak the user's location only consider **K**-anonymity and **L**-diversity. This paper presents a novel personality privacy-preserving cloaking framework for the protection of sensitive positions on road-network environment. In our scheme, a Voronoi-partition graph is first learned from an urban network, and a Dominance Date Center (DDC) is introduced to take charge of the vertex's Voronoi-partition (dominance space) data. Then, the θ-security semantics is introduced to measure the degree of sensitive semantics leakage. Thus, a lightweight agent running in the client can contract with DDC and process the sensitive semantics-aware cloaking algorithm to generate a cloaking region to meet **K**-anonymity and θ-security semantics. Final, not the anonymizer, but the client agent access direct into the LSP.*

Keywords: *Location-based Services, location semantics-aware, **K**-anonymity, **L**-diversity, θ-security, Voronoi-partition*

1. Introduction

Recently, location-based services (LBS) are becoming increasingly popular with the growth of location aware technique. LBS can provide services for mobile users according to their location, including place of interesting (POI) finders ("Where is the nearest hospital?"), friends alarms ("Remind me when my friends are 10 miles around me?"), transportation applications ("What is the traffic condition on this way?"), and so on. Mobile users obtain such services by issuing queries together with their location information to the LBS providers (LSP). More accurate location, the higher the quality of services (QoS), however, the more location-privacy leaked. This is a trade-off between location-privacy preserving and QoS.

K-anonymity [1] and *L*-diversity [2] have been putted forward to protect location-privacy on road networks. *K*-anonymity spatial region (*K-ASR*) [3-9] can blur the user's exact location into spatial region, which includes '*k*-1' other users. *L*-diversity can promote that *K-ASR* should contain '*l*' different road segments, that should be difficult for the adversary to link a specific user with a specific road segment with high certainty [8, 10-11].

Generality, the cloaking region could contain some semantic places which may be sensitive to the user, so the adversary can infer the user's semantic meaning together

ISSN: 1738-9976 IJSIA

with other information. For example, it is provided that the semantic places contained in the user's cloaking region are only one semantic type (*e.g.*, hospital), which is sensitive for her, the adversary could infer her health conditions. Obviously, it will be not work for semantic-privacy protection only to consider '*k*' different users and '*l*' different road segments. The issues of location semantic breach have already caused wide public concern [11, 17-19].

Unfortunately, existing semantics-aware cloaking methods are unthoughtful in the sense that: 1) they could not be adapted to road networks in which users can move with restrictions; 2) they do not consider individual difference. That is, whether a semantic place is sensitive or not relies on the user personal feeling, for example, one could think that a school or a hospital is his sensitive place, while another could think that a bar is sensitive for her; 3) almost all semantics-aware cloaking regions are formed by the trust anonymizer, which can be a bottleneck of the cloaking system and the attacking target of the adversaries. Therefore, a sensitive semantics-aware personality cloaking is needed to further foster on road networks.

In this paper we address all these requirements and propose a novel personality location-privacy protection technique, which protects the sensitive semantics from an adversary on road networks. In summary, the primary contributions of this paper are:

- This paper proposes Voronoi-partition diagram learned from an urban network, whose vertex is an intersection or a semantic place. The Dominance Date Center (DDC) is introduced to take charge of the real-time users' number in the vertex's Voronoi-partition (dominance space). While the cloaking region is consist of one or more Voronoi-partition, which have already consider the diversity of road segments, therefore, this paper mainly focuses on how to protect the sensitive semantics.
- This paper proposes a personality method that protects the user's sensitive semantics on road networks. Our idea is to let a user express her privacy requirements by specifying some types of sensitive semantics. In this paper, not the number of place type, but the popularity ratio is introduced to measure the degree of semantic diversity. A space area is considered as the user's cloaking region, if the popularity of sensitive semantics customized by the query user is not more than a threshold θ in total popularity of semantics in the space area.
- This paper proposes a cloaking method without involving the trusted anonymizer. Our idea is to let a lightweight client agent running in user contracts with the DDC through providing a user-chosen suitable area (A_{suit}), and then the DDC returns the dominance region information of corresponding A_{suit}. Final, not the anonymizer, but the client agent computes the cloaking region and access direct into the LSP.

The remainder of this paper is organized as follows. Section 2 surveys related work. Section 3 describes the background and limitation of location privacy protection, formally definition the semantic-security requirement. Section 4 gives the system architecture and the attack model. Algorithms are provided in Section 5. Section 6 gives the evaluation results of our proposed algorithms. Section 7 concludes and presents the future work.

2. Related Work

Previous works in location privacy-protection can include false dummies [12], space transformation [13], and spatial cloaking [1-9]. In these three techniques, the most popular preserving mechanism is spatial cloaking, which uses a cloaking region including the user and '*k*-1' other users to be instead of the query user's exact location. Casper [5], Interval [4] and Hilbert-based cloaking [9] are the typical anonymous technique.

Unfortunately, these mentioned cloaking techniques are designed for Euclidean space, and not consider the diversity of road segment. As a result, X-star [14] and other works [15-16] blur the user's exact location into a set of segments, and the number of the segments is the degree of *L*-diversity. In reality, the cloaking region can contain some semantic places together with road segments, and the semantic information may leak the user's privacy. PrivateGrid [8] proposes combining *l*-places, but it does not distinct between sensitive and non-sensitive places. All mentioned cloaking region is not *l*-type diverse, for example, all places included in the cloaking region may be the same type (*e.g.*, hospital), and therefore, it is vulnerable to a *location similarity attack*. Existing works [11, 17-18] have already started to focus on the issues of location semantic breach. Unfortunately, they only taken into account confusing (*l-1)*-type semantics together with sensitive semantics, not consider that the popularity of every place has diversity. For example, the cloaking region contains three different semantics (*l=3*), one of which is dominance (*e.g.*, school, which is the user's sensitive semantics), then the user might be associated with the dominant semantics with high probability, and so the privacy is disclosed. Therefore, it is needed that an effective method to protect location semantics. The work [19] proposes mining the place semantics using EMD to avoid location semantic leakages, but it does not consider the road networks environment. The work [20] presents a semantic location cloaking model for location sharing under road-network constraints, but it relies on the trusted anonymizer. So, it is needed that a semantic protection technique suitable for the road-network.

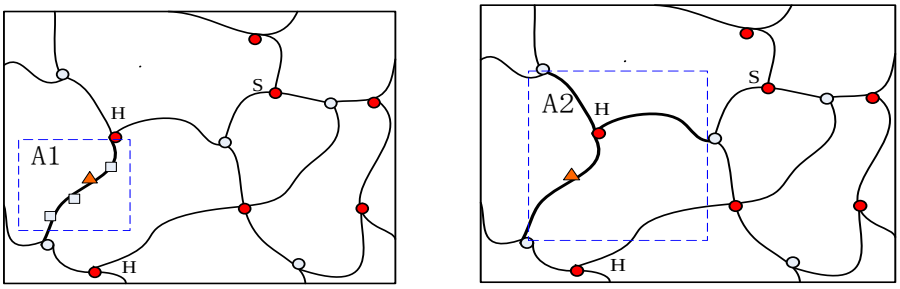
In architecture model, existing location privacy protection schemes can be classified into two categories: (1) three-tier framework [1-12]. In this framework, the trusted anonymizer located between the user and the LSP blurs the user's exact location and transforms the query candidates. (2) two-tier framework [13, 21, 27, 22-26]. In this framework, the user can directly contract with the LSP through using space transformation [13], Private Information Retrieval (PIR) [21], probabilistic anonymity [26] or peer-to-peer (P2P) model [22-26]. Due to that the trusted anonymizer is easy to be an attack target and performance bottlenecks, therefore, this article adopts the two-tier framework.

3. Mining Location Semantics

3.1. Background and Limitations

Figure 1 depicts an example of *location similarity attack*. It is supposed that the orange triangle represents a query user, the white quadrangle represents a mobile user, the red and white circle represent a semantic place and an intersection respectively (*H*: hospital, *S*: school). Figure 1 (a) shows that the clocking region (A_1) meet *K*-anonymity *(K*=4), but it contains only one road segment, it is vulnerable to *location similarity attack*. To conquer this, A_2 included 3 road segments. But it contains only one semantic place (i.e. *H*), which is sensitive to the query user, so it is still vulnerable to *location*

similarity attack. So, both *K*-anonymity and *L*-diversity schemes are vulnerable to *location similarity attack*. It is desirable a cloaking method for preserving location semantics privacy. Thinking about these mentioned above, we first give the definition of the Voronoi-partition road network as follows.



(a) *K*-anonymity(*K*=4) (b) *L*-diversity(*L*=3)

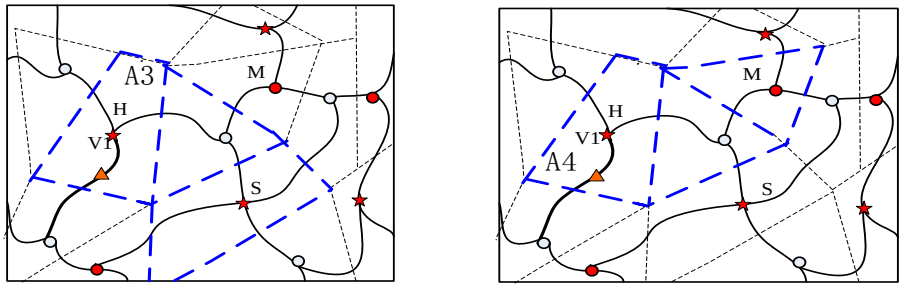
Figure 1. An Example of Location Similarity Attack

Definition 1 Voronoi-partition road network. A Voronoi-partition road network *G= (V, E, DR(v))* learned from undirected urban network, where

1) $V = V_P \bigcup V_I$ is the set of vertices with $v \in V_P$ representing a semantic place and $v \in V_I$ representing a road intersection.

2) $E \subseteq V \times V$ is the set of edges, and $e = (u, v) \in E$ $(u, v \in V_P or V_I)$.

3) *DR(v)* is the dominance region of the vertex *v* in the two dimensional road network, that is *DR(v)*= $\{ x : d(x,v) \le d(x,w), \forall w \ne v, (w,v) \in V \}$, where *d(x, v)* is the network distance from *x* to *v*, not the Euclidean distance from *x* to *v*. Note that a Voronoi-partition is on behalf of one vertex's dominance region.



(a) including two sensitive semantics (b) including one sensitive semantics

Figure 2. Another Example of Location Similarity Attack

Figure 2 shows an example of Voronoi-partition road network. It is supposed that red star is the sensitive place to the query user *U* {*H*: hospital, *S*: school}, and the query user's location locate in the dominance region of v_1, that is *DR* (v_1). Due to v1 is sensitive for the user, *DR* (v_1) should be expanded, and its result is A_3 or A_4. In Figure 2 (a), A_3 is contained the dominance region of one road intersection and two semantic places, which are sensitive for *U*, so it is vulnerable to *location similarity attack*. Therefore, it is needed to balance the sensitive semantic differences of the cloaking

region. As shown in Figure 2 (b), because that A_4 also contains a non sensitive semantics of U (M: mall), *location similarity attack* is decreased obviously.

3.2. Location Semantic Security

3.2.1. The Popularity of Semantic Places: To determine a cloaking region is semantic security for the user, it is important to calculate how much semantic information was leaked, but it is very difficult to infer that the adversary can obtain location semantics from a cloaking region. Often, the location semantics is associated with the service type, which can be first classified according to the collection of point of interest (POI), such as hospital, school, restaurant, supermarket, etc. Due to the popularity of each service is different, so the amount of semantics leaked is different. Figure 2 shows that A_4 contains two semantic places {H, M}, and if the popular degree of hospital is higher than mall, that is, the sensitive semantics is the dominance in the total location semantics, so it is apparently for the adversary to associate the sensitive semantics with the user with a high probability. Therefore, it is very important to get a semantic security cloaking region, and the entropy is firstly introduced to measure the popularity of different service in this article.

Definition 2 Popularity. Let v_p be a semantic place and $S(v_p)=\{u_1,u_2,...,u_m\}$ be the set of users who have footprints in v_p. Let n_i ($1 \le i \le m$) be the number of footprints that user u_i has in v_p, and $N=\sum_{i=1}^{m} n_i$. We define the entropy of v_p as $E(v_p)=-\sum_{i=1}^{m}\frac{n_i}{N}\log\frac{n_i}{N}$, and the popularity of v_p as $P(v_p)=2^{E(v_p)}$.

Obviously, the popularity of a semantic place embodies its average intensity, for example, the popularity of mall is usually greater than the office. To distinguish a semantic place and a road intersection, popularity of a road intersection is often set to 0.

3.2.2. Privacy Requirement: Let $PT=PT_{NS}\bigcup PT_S$ be a set of the total place types, PT_S be a set of the user-defined sensitive service types and PT_{NS} is a set of nonsensitive service types. Let $V_P=V_{SP}\bigcup V_{NSP}$ be a set of semantic places with $v_{sp}\in V_{SP}$ representing a sensitive place and $v_{nsp}\in V_{NSP}$ representing a nonsensitive place.

Definition 3 Θ -Security Cloaking Area. If a cloaking region (CR) satisfies $div_{CR}=\frac{\sum_{v_{sp}\in V_{SP}\wedge v_{sp}\in CR}P(v_{sp})}{\sum_{v_p\in V_P\wedge v_p\in CR}P(v_p)}\le\theta$, we denote this cloaking region CR as a θ-security cloaking area.

In definition 3, θ-security level describes the disclosing level from the adversary's point of view. The smaller θ is, the higher the security level of cloaking region is.

To avoid *anonymity attack* and *location similarity attack*, it is hoped that the cloaking region should meet the demand of K-anonymity and θ-security.

According to the demand of θ-security, it is supposed that all service types have the same popularity ($P(v)$=0.1, where $v \in V_p$), the user's sensitive places set is {H, S}, and θ =0.5. Such that, the semantic diversity of A_3 is calculated as $div_{A3} == \frac{0.1+0.1}{0.1+0.1} = 1 > 0.5$, so it does not meet the requirement of θ-security cloaking area, while the semantic diversity of A_4 is calculated as $div_{A4} = \frac{0.1}{0.1+0.1} = 0.5 \leq 0.5$, so A_4 is the θ-security cloaking area. In reality, the popularity of hospital is different with the one of mall, assuming that the former is higher than the latter, so A_4 does not meet the degree of θ-security. Therefore, we need a sensitive semantics-aware cloaking algorithm to find a θ-security cloaking area.

4. System Model

Figure 3 shows this system architecture, which adopts the architecture of the ref. [31]. This framework is two-tier without the trusted anonymizer, a DDC is introduced to take charge of the number of users in real-time for every vertex's dominance space. The user initiates the query by choosing a suitable area (A_{suit}) where he/she locates and sends A_{suit} to the DDC, and then the DDC responds with the dominance region information of corresponding A_{suit} (DR_{Asuit}). Thus, according to the response, the client engine will select one or more Voronoi-partitions to form a secure cloaking region (CR) and direct access to the LSP. In the scheme, the exposed location is A_{suit}, which is a finite large area selected by the user, that is, the user's exact location will be not leaked to any others. Moreover, the cloaking algorithm is executed by the client engine; therefore, a high efficiency and low overhead cloaking algorithm is needed.

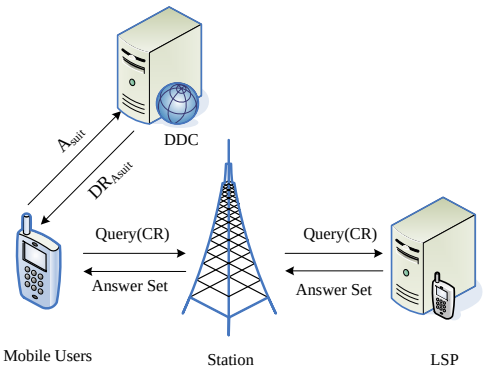


Figure 3. System Structure

Attack model. It is considered that the LSP and DDC are honest but curious and both of them can be compromised by attackers, thus, attackers are aware of the location and the queries submitted by users, *i.e.*, A_{suit} and *query (CR)*. Note that attackers are not only interested in the querier's actual location, but also interested in the location semantics contained in the querier's cloaking region. Therefore, this paper aims to perform a cloaking mechanism for protecting users' location privacy and semantic privacy.

5. Sensitive Semantics-aware Cloaking Algorithm

From the above analysis, there are two keys for protecting mobile users' privacy, the one is *K*-anonymity, and another is θ-security semantics. Aiming at this problem, this paper presents a sensitive semantics-aware cloaking algorithm to obtain a security cloaking region, which can meet the two privacy requirement. Before executing cloaking algorithm, the query user should put forward a privacy profile about: 1) a set of sensitive place types $PT_S = \{pt_s^1, pt_s^2, \cdots pt_s^n\}$, 2) the level of *K*-anonymity, 3) the level of θ-security semantics. Thus the client agent can contract with the DDC and obtain real-time users' number in DR_{Asuit}.

Algorithm 1 first determines the query user's dominance region(*DR*), which is *U*'s initial *CR*, at the same time, the vertex (*w*) and the user number (*kNum*) of the corresponding *DR* can be obtained (line 1). If the service type of *w* ($PT(w)$) is not one of PT_S' (*i.e.*, *w* is an intersection or a nonsensitive place), the algorithm 2_1 will be called (line 4), otherwise, the algorithm 2_2 will be called (line 5).

Algorithm 1 Sensitive Semantics-Aware Cloaking Algorithm

input: A *U*'s location loc_u, a DR_{Asuit}, a privacy profile $pp = \{PT_S, K, \theta\}$, and a maximum number of iterations maxLoop.

output: θ-secure cloaking region

1) (*CR*, w, kNum,)= GetInitialCR (loc_u, DR_{Asuit});
2) V'={w};
3) **if** $PT(w) \notin PT_S$ **then**
4) call algorithm 2_1(DR_{Asuit}, *CR*, kNum, V', *pp*, maxLoop);
5) **else** call algorithm 2_2(DR_{Asuit}, *CR*, kNum, V', *pp*, maxLoop);
6) **end if**

In algorithm 2_1, if *k*Num meets the *K* requirement, the *CR* will be returned (line 1-2). If not, the algorithm will search each possible direction (link) of *CR* in DR_{Asuit} and obtain corresponding adjacent points (v_{link}) (line 6), and next, just only dominance region of nonsensitive places or road intersections can be joined into the cloaking region (line 9). This aim is to satisfy that the cloaking region does not contain sensitive place, that is, the algorithm does no need to consider the semantic diversity of cloaking region. If all direction pathways are searched in one round, the demand of *K* is yet not to be met, then the algorithm continue to the next round of searching until reaching maximum loop times (maxLoop). If only sensitive places could be found in one loop, the algorithm will chose one sensitive place whose popularity degree is smallest among V_S to extend and call the algorithm 2_2 (line 16-17).

Algorithm 2_1 Cloaking from Intersection or Nonsensitive Place

Input: DR_{Asuit}, *CR*, kNum, *V'*, *pp*, maxLoop
output: θ-secure cloaking region

1) **if** kNum>=*K* **then**
2) return *CR*;
3) **end if**
4) **for** *i*=1 to maxLoop **do**

```
5)      kNum_before = kNum;    V_S = Φ;
6)      for each (link, v_link) ∈ GetPossibleLinks (CR, DR_Asuit) do
7)        if PT(v_link) ∈ PT_S then
8)          V_S = V_S ∪ {v_link} ;
9)        else (CR,V', kNum)= ExtendCR (CR, v_link) ;
10)       end if
11)       if kNum>=K then
12)         return CR;
13)       end if
14)     end for each
15)     if kNum_before =kNum then
16)       (CR,V', kNum)= ExtendCR (CR, GetMinPop (V_S )) ;
17)       call algorithm 2_2(DR_Asuit, CR, kNum, V', pp, maxloop-i);
18)     end if
19) end for
```

Algorithm 2_2 will first search each possible direction (*link*) of *CR* in turn and obtain corresponding adjacent points (v_{link}) (line 4), then the dominance region of v_{link} which belongs to nonsensitive places can be added to cloaking region, and the popularity diversity should be calculated (line 6-7). If the θ-security and *K*-anonymity can be met, the CR can be returned (line 8-9), otherwise, continue to search. In one loop, if nonsensitive places is not exist (line 18), the dominance region of any intersection is priority joined in (line 20). If there is neither nonsensitive place nor intersection in one loop, the algorithm can not but chooses a sensitive place whose popularity degree is smallest among V_S to join in (line 21).

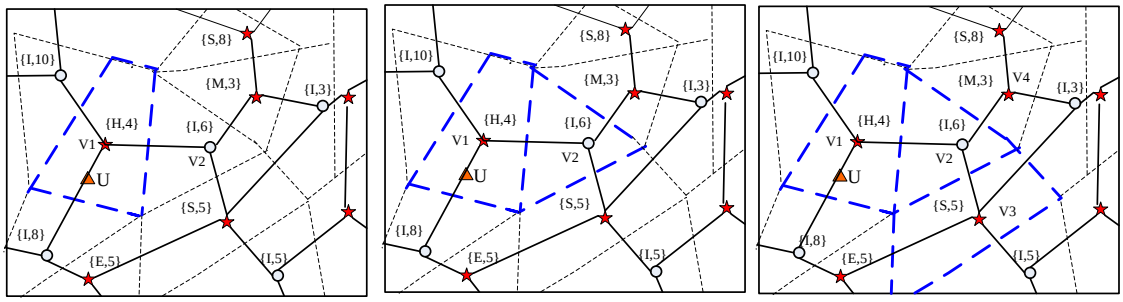
Algorithm 2_2 Cloaking from Sensitive Place

```
input: DR_Asuit, CR, kNum, V', pp, maxloop
output: θ-secure cloaking region
1)    for i=1 to maxLoop do
2)      kNum_before = kNum;
3)      V_I = V_S = Φ;
4)      for each (link, v_link) ∈ GetPossibleLinks (CR, DR_Asuit) do
5)        if PT(v_link) ∈ PT_NS then
6)          (CR,V', kNum)= ExtendCR (CR, v_link) ;
7)          div_CR =PopDiv (CR);
8)          if ( div_CR ≤ θ and kNum>=K) then
9)            return CR;
10)         end if
11)       else
12)         if PT(v_link) ∈ PT_S then
13)           V_S = V_S ∪ {v_link};
```



```
14)          else  V_I = V_I ∪ {v_link};
15)          end if
16)       end if
17)     end for each
18)     if (kNum == kNum_before)  then
19)        if(V_I ≠ Φ )   then
20)           (CR,V', kNum)= ExtendCR (CR, GetOne(V_I )) ;
21)        else      (CR,V', kNum)= ExtendCR (CR, GetMinPop (V_S )) ;
22)        end if
23)     end if
24)   end for
25)   return CR ;
```

Figure 4 depicts an example of the algorithm about privacy profile of PP_1= {{*S*}, *K*=7, θ =0.5} and PP_2={{*H*,*M*},*K*=7, θ =0.5} respectively. In Figure 4, a Voronoi-partition along with its vertex's type and the users' number are marked. The hypothetical popularity for type of places is as following: {School(S): 0.2, Hospital(H): 0.15, Office(O):0.25, Entertainment(E):0.15, Mall(M):0.15, Park(P):0.15, Intersection(I): 0}. If *U*'s privacy profile is described as PP_1, Figure4(a) shows that the initial CR(*U*)={DR(v_1)} and $PT(v_1) = H \notin \{S\}$, *CR.K*=4<7 (the *U.K* =7), so continue to call algorithm 2_1. Figure 4(b) depicts that the *CR* is extended with the dominance region of v_2 (v_2 is an intersection), because of *CR.K*=4+6>7, so it meets the *U*'s privacy profile, the *CR(U)={DR(v_1)+DR(v_2)}* will be returned. If *U*'s privacy profile is described as PP_2, Figure 4(a) shows $PT(v_1) = H \in \{H, M\}$, so it continues to call algorithm 2_2. In searching step 1, due to the type of every possible adjacent vertex is intersection, any intersection (*e.g.*, v_2) is selected (Figure 2(b)), *i.e.*, *CR(U)={DR(v_1)+DR(v_2)}*, so continue to search. In searching step 2, all possible adjacent vertex is {v_3,v_4}, $PT(v_4) = M \in \{H, M\}$, $PT(v_3) = S \notin \{H, M\}$, so *DR*($v_3$) will be added to *CR(U)*, that is, *CR(U)={DR(v_1)+DR(v_2)+DR(v_3)}*, meanwhile *CR.K*>7 and $CR.div = \frac{0.15}{0.2 + 0.15} \le \theta = 0.5$, so *U*'s privacy profile is met, the *CR(U)* will be returned.



(a) Get initial CR (b) Add v_2 's dominance region (c) Add v_3 's dominance region

Figure 4. An Example of Sensitive Semantics-aware Cloaking Algorithm for PP_1={{*S*},*K*=7, θ=0.5} or PP_2={{*H*,*M*},*K*=7, θ=0.5}

6. Experiments

In this section, we evaluate the performance of the proposed sensitive semantics-aware cloaking algorithm (donated as SA), three distinct personalized privacy profiles are pp_1=NULL (donated pp_1-SA), pp_2= {Entertainment} (donated pp_2-SA) and pp_3= {Hospital, Office} (donated pp_3-SA) respectively. For comparison purpose, we have implemented one network expanding approach, term as EA, which forms cloaking region considering *K*-anonymity and *L*-diversity (*L* road segments, *L*=3).

6.1. Experimental Setting

We first pick a real road map of Oldenburg, Germany (from OpenStreetMap), which contains 6,105 nodes and 7,035 edges, and its area is about 15×15 km^2, and then we process the raw data to obtain the Voronoi-partition city network according to our definition: one edge is behalf of a road, the junction of edges is the vertex, which may be an intersection or a semantic place, and a Voronoi-partition is a vertex's dominance region. It is assumed that 10,000 mobile users randomly walk over road network, and one-tenth of them issue query requests. In this experiment, we just discuss 6 types of semantic place, whose popularity can be computed as definition 2, to be simple, these popularity is assumed as Section 5. The experimental data is given as Table 1.

Table 1. Parameter Settings

Parameters	Default values	Range
K- anonymity	6	[3,12]
θ	0.4	[0.2,0.8]
Number of semantic places	600	[300,1200]
Place types(counts)	School(S:32), Office(O:87) , Hospital(H:36), Market(M:50), Entertainment(E:29)	
maxLoop	5	5

6.2. Experimental Results

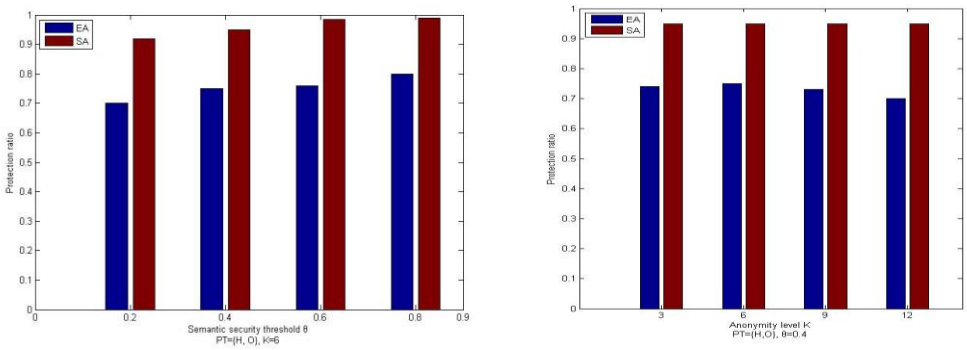


Figure 5. Protection level

1) **Protection Level.** This measures the disclosing level of sensitive-attack, that is, the adversary would gain location semantic information from a cloaking region. To measure this, we introduce the average protection ratio about the number of θ-security cloaking regions to the number of total cloaking regions. In order to compare the

semantic security of algorithm EA and SA, it is uniformly assumed that the user's sensitive profile is $PT= \{H, O\}$ for both algorithms. Figure 5 shows the security level to the sensitive-attack with respect to varying the θ- security level from 0.2 to 0.8, and K-anonymous level from 3 to 12. Because that SA considers the semantic-security, while EA does not, as shown in Figure 5 the protection ratio of EA is much lower than the one of SA, which is very close to 1 and is almost not affected by K level. So it is clear that our method provides better safety when the costs for enforcing the location privacy are the same.

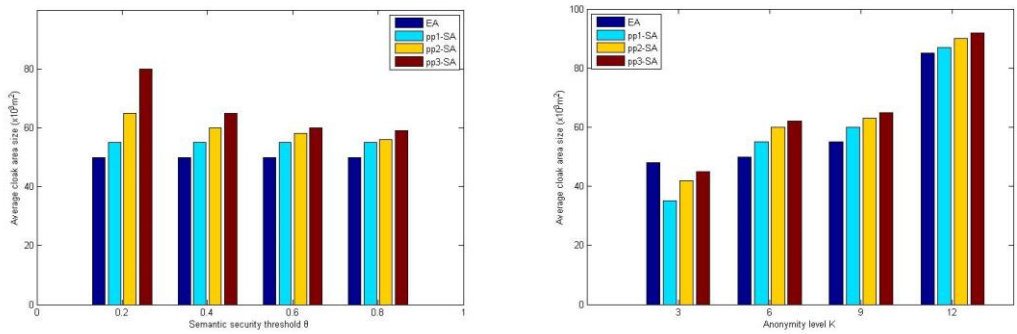


Figure 6. The System Performance

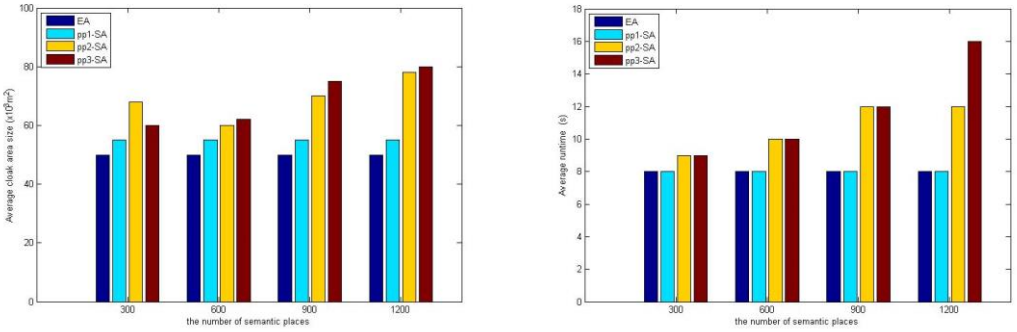


Figure 7. Scalability

2) Cost Awareness. This is the size of average cloaking area. Figure 5 depicts that performance results with respect to varying θ-security threshold level from 0.2 to 0.8, and K-anonymous level from 3 to 12. Figure 6(a) indicates that pp_1-SA and EA are not affected by θ level, while the average size of pp_2-SA and pp_3-SA are higher than one of the previous two. This is because that EA and pp_1-SA only consider the K value, and pp_2-SA and pp_3-SA need to expand more number of Voronoi-partition to meet the θ level. Figure 6(a) also gives that the cloaking area size decreases when the θ increases. This is because if θ-security level is low, more nonsensitive positions will be need to be expanded, thus the size of cloaking region is larger. In Figure 6(b), it is clear that the cloaking area size of EA is higher than pp_1-SA when K=3. This is because that the area size of a Voronoi-partition is lower than the 3-diversity road segments. Figure 6(b) also gives that the cloaking area size increases when the K increases. It is clear that our method does not increase too much cost when the security is the same.

3) Scalability. This measures the effectiveness and efficiency performances about the increasing number of semantic places. For scalability tests, the number of each semantic type is proportional increased, thus the total number of semantic places is increased. Figure7 shows that average cloaking area size and average runtime with respect to varying number of semantic places from 300 to 1200. In these tests, the value of K and θ is set to 6 and 0.4 respectively. Because that EA and pp_1-SA do not concern semantic-security, both of them are not affected by this change. As shown in Figure 7 pp_2-SA and pp_3-SA have certain growth with the increasing of the number of semantic places. But this growth is acceptable for the scalability of our algorithm.

7. Conclusion

In this paper, we present a novel personality location privacy protection technique, which protects the sensitive semantics from an adversary for road networks. The main idea of this scheme is to expand the vertices' dominance region to realize K-anonymity and θ-security semantics cloaking. It is important to note that the system does not rely on the anonymity server, but introduces a DDC, which provides the data information of every vertex's Voronoi-partition to the user. The client will run an efficient cloaking algorithm to form a secure cloaking region and will contract directly with the LSP. Therefore the scheme guarantees that the disclosure information is minimize. Moreover, the experiments indicate that our scheme can reach high level of location privacy. However, due to the agent running in the client communication with the DDC with a large area, that can consume the client's bandwidth. So, in the future, we can focus on cloaking scheme for protection location semantic security with low bandwidth consumption.

Acknowledgements

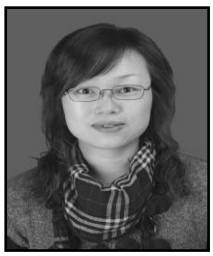
This work was supported by Key Project on the Integration of Industry, Education and Research of Guangdong Province (Grant No. 2012B091000054), and Sichuan Department of Education (Grant No.13ZB0152). This work was also partly supported by the National Nature Science Foundation of China under Grant (No.61373163).

References

[1] L. Sweeney, "K-anonymity: A model for protecting privacy", International Journal of Uncertainty Fuzziness and Knowledge Based Systems, vol. 10, no. 557, **(2002)**.
[2] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam, "L-diversity: Privacy Beyond k-Anonymity", Proceedings of ACM Transactions on Knowledge Discovery from Data (TKDD), **(2007)**, pp. 1-52.
[3] B. Gedik and L. Liu, "Location Privacy in Mobile Systems. A Personalized Anonymization Model", Proceedings of 25th IEEE International Conference on Distributed Computing System, Columbus, OH, **(2005)**.
[4] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking", Proceedings of 1st International Conference on Mobile System, New York, **(2003)**, pp. 31-42.
[5] F. M. Mohamed, C. Y. Chow and G. A. Walid, "The new casper: Query processing for location services without compromising privacy", Proceedings of 32nd International conference on Very Large Data Bases, ACM Press, **(2006)**, pp. 763-774.
[6] T. Xu and Y. Cai, "Location anonymity in continuous location-based services", Proceedings of 15th ACM Symposium on Advances in Geographic Information Systems, New York, **(2007)**.
[7] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location- based services", Proceedings of IEEE INFOCOM 27th International Conference of the Computer and Communications Societies, Phoenix, AZ, **(2008)**, pp. 547-555.

[8] B. Bamba, L. Liu and P. Pesti, "Supporting anonymous location queries in mobile environments with PrivacyGrid", Proceedings of the 17th International Conference on World Wide Web, New York, **(2008)**, pp. 237–246.
[9] P. Kalnis, G. Ghinita and K. Mouratidis, "Preventing location-based identity inference in anonymous spatial queries", Proceedings of IEEE Transactions on Knowledge and Data Engineering, **(2007)**, pp. 1719-1733.
[10] T. Wang and L. Liu, "Privacy-aware mobile services over road networks", Proceedings of the VLDB Endowment, **(2009)**, pp. 1042-1053.
[11] M. Xue, P. Kalnis and H. Pung, "Location Diversity: Enhanced Privacy Protection in Location Based Services", Location and Context Awareness (LoCA), **(2009)**, pp. 70-87.
[12] H. Kido, Y. Yanagisawa and T. Satoh, "An Anonymous Communication Technique using Dummies for Location-based Services", Proceedings of IEEE International Conference on Pervasive Services, ICPS, **(2005)**.
[13] A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy", Proceedings of the International Symposium on Spatial and Temporal Databases, **(2007)**.
[14] T. Wang and L. Liu, "Privacy-Aware Mobile Services over Road Networks", Proceedings of the International Conference on Very Large Data Bases, **(2009)**.
[15] C. Y. Chow, M. F .Mokbel and X. Liu, "Query_aware Location Anonymazation for road networks", GeoInformatica. vol.15, **(2011)**, pp.571-607.
[16] Y. K. Kim and A. Hossain, "Hilbert-order based spatial cloaking algorithm in road network", Concurrency and Computation: Practice and Experience, vol.25, **(2013)**, pp. 143-158.
[17] M. Damiani, E. Bertino and C. Silvestri, "The PROBE Framework for the Personalized Cloaking of Private Locations", Transactions on Data Privacy, vol. 3, **(2010)**, pp. 123-148.
[18] Z. Xiao, J. Xu and X. Meng, "p-Sensitivity: A Semantic Privacy-Protection Model for Location-based Services", Proceedings of International Conference on Mobile Data Management Workshops, **(2008)**.
[19] L. Byoungyoung, Oh. Jinoh and Y. Hwanjo, "Protecting location privacy using location semantics", Proceedings of the 17th ACM SIGKDD, **(2011)**, pp. 1289-1297.
[20] E. Yigitoglu and M. L. Damiani, "Privacy-Preserving Sharing of Sensitive Semantic Locations under Road-Network Constraints", Proceedings of International Conference on Mobile Data Management, **(2012)**, pp. 186-195.
[21] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K. L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary", Proceedings of the ACM International Conference on Management of Data, SIGMOD, **(2008)**.
[22] G. Ghinita, P. Kalnis and S. Skiadopoulos, "Mobihide: A mobile peer-to-peer system for anonymous location-based queries", J. Advances in Spatial and Temporal Databases Lecture Notes in Computer Science, vol. 4605, **(2007)**, pp. 221-238.
[23] G. Ghinita, P. Kalnis and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems", Proceedings of International World Wide Web Conference, New York, **(2007)**, pp. 371-380.
[24] C. Y. Chow, M. F. Mokbel and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location based service", Proceedings of 14th annual ACM international symposium on Advances in geographic information systems, New York, **(2006)**, pp. 171-178.
[25] W. S. Ku, R. Zimmermann and H. Wang, "Location-based spatial query processing with data sharing in wireless broadcast environments", Proceedings of International Conference on IEEE Transactions on Mobile Computing, IEEE Press, **(2008)**, pp.778-791.
[26] C. Y. Chow, M. F. Mokbel and X. Liu, "Spatial Cloaking for Anonymous Location-based Services inMobile Peer-to-Peer Environments", J. GooInformatica, vol. 15, **(2011)**, pp. 351-380.
[27] S. I. Ahamed and M. M. Haque, "A Novel Location Privacy Framework without Trusted Third Party Based on Location Anonymity Prediction", Proceedings of Research in Applied Computation Symposium, vol. 12, **(2011)**, pp. 24-34.

Authors



Min Li, was born in Sichuan, China, in 1978. She received the M.S. degree in the University of Electronic Science and Technology of China, in 2005. She is currently working toward the Ph.D. degree in computer science at UESTC. Her current research interests include wireless sensor networks, privacy protection, specifically the location privacy in LBS.

Zhiguang Qin, received Ph.D degree from the University of Electronic Science & Technology of China. Now he is a professor, dean of Computer Science & Engineering Department, director of Computer Application Key Lab in Sichuan Province, member of IEEE. Currently his main research interests concern is the security of the networks.

Cong Wang, received the B.S. and M.S. degrees from Southwest University of China, Chong-qing, China. Currently he is pursuing the Ph.D. degree in computer science at the University of Electronic Science & Technology of China. His main research interests are the applications of machine learning techniques to computer networking problems, specifically the prediction of latency in large-scale networks.