A Spatial Cloaking Framework Based on Range Search for Nearest Neighbor Search

Hyoungshick Kim

Computer Laboratory,
University of Cambridge, UK
hk331@cam.ac.uk

Abstract. For nearest neighbor search, a user queries a server for nearby points of interest (POIs) with his/her location information. Our aim is to protect the user's sensitive information against adversaries including the location-based service itself. Most research efforts have elaborated on reasonable trade-offs between privacy and utility. We propose a framework based on range search query without a trusted middleware. We design a query processing algorithm for the minimum set of candidate POIs by computing the local Voronoi diagram relevant to the cloaked region. Contrary to common belief that cloaking approaches using range search incur expensive processing and communication cost, the experimental results show that the framework incurs reasonable processing and communication overhead even for large cloaked regions.

Keywords: Location Anonymity, Spatial Cloaking, Query Privacy, Voronoi Diagram, Nearest Neighbor Search.

1 Introduction

With the rapid evolution of mobile computing, location sensing, and wireless networking, geospatial applications are quickly growing in popularity [1]. Location-based services are personalized services in geospatial applications to provide useful location information for a given position. One of fundamental location-based services is to search the nearest neighbor to user location. A user can ask the closest POIs (e.g., hospital, hotel, or gas station) to her current location.

For personalized location-based services, a user must report her location. Location is an especially sensitive type of personal information. The information about user location may be clue to infer the user's sensitive information such as health, private lifestyle, and personal preference. For example, an employer may check on her employee's behaviour by knowing the places the employee visits and the time of each visit, the personal medical records can be inferred by knowing which the clinic a person visits, or someone can stalk the locations of her acquaintances. Therefore location privacy will be one of the key issues to deploy location-based services although they provide helpful and intelligent results.

As an intuitive approach to preserving location privacy, we enlarge an exact user location into a cloaked region so that it is infeasible to infer the user's exact

J. Garcia-Alfaro et al. (Eds.): DPM 2009 and SETOP 2009, LNCS 5939, pp. 93–105, 2010.

location from the cloaked region. Sensitive information about an individual user location can be protected by controlling the level of detail of a cloaked region including user location. Previously, it was believed that spatial cloaking solutions using range search query incur expensive processing and communication cost for large number of POIs. However, we believe that range-based spatial cloaking can be practically applicable since recent growth in networking technology have enabled communication to transmit high bandwidth data (e.g., map data) in real time.

We propose a range-based framework that does not rely on an external anonymizer, which collects the location information of users and anonymizes their queries. In practice, it is hard to assume a trustful mediator between users and location services. Since most existing location-based services are based on a standard client-server architecture, it is desirable for two-tier spatial cloaking where the cloaked region can be constructed and sent by the user directly without dependency of an external party.

In range-based spatial cloaking, the most challenging issue is to minimize processing and communication overheads due to range search. There is an inherent trade-off between user privacy and service utility. A larger cloaked region implies higher guarantees for location privacy, but it also requires high computational and communication costs.

Interestingly, given a cloaked region including user location, finding the nearest POI to the user location cannot be acheived by range search with a fixed region. Fig. 1 illustrates that the problem of range search with a fixed region. In this example, the nearest POI to the user location u is p_1. The conventonal range search algorithms with a fixed region, that do not consider outer points of the region, cannot guarantee the nearest POI to user location.

Therefore, we should also consider outer points of a cloaked region. We observe that it can be transformed to finding intersections of Voronoi cells for POIs with a cloaked region since the user position can be uniformly located at the cloaked region. This also means that the minimum size of the candidate answer results in $\Omega(k)$ where k is the number of the Voronoi cells which intersect with a cloaked region. Our query processing algorithm is based on computation of the intersections of Voronoi cells with a cloaked region.

When the locations of POIs (e.g., buses) are dynamically changed or the server's storage is limited to maintain the overall Voronoi diagram, the precomputed Voronoi diagram cannot be used. Our objective is to avoid computing

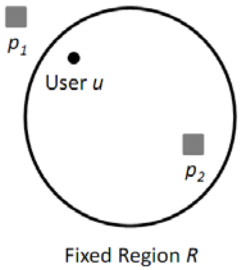


Fig. 1. A counter-example to range search with a fixed region

the global Voronoi diagram for a large data set, which is forbiddingly costly in terms of CPU and memory. Therefore we design the online computation of the candidate neighbors using the local Voronoi diagram relevant to a cloaked region. We show that the computed local Voronoi diagram always successfully include the correct query answer.

In addition, we suggest a heuristic sampling method to provide an approximate answer statistically when a limited communication bandwidth is required for nearest neighbor search. A reasonable approximate sample set can be also retrieved using the intersections of Voronoi cells depending on the maximum permitted communication cost.

The proposed framework is simple and can be integrated into a general server-client architecture without a trusted middleware. Empirical studies show reasonable communication cost in real datasets even if a user requires high privacy.

The remainder of the paper is organized as follows. In Section 2, we review the related work. In Section 3, we introduce data structure, notations, and threat model. In Section 4, we propose a framework based on computation of local Voronoi diagram. The experimental results in terms of communication and computational costs, are analysed in Section 5. Finally, we conclude the results and suggest some directions for future research in Section 6.

2 Related Work

In spatial cloaking, user location is enlarged into a cloaked region that is then used for querying the server. One of the main goals in those studies is to provide k-anonymity. The concept of k-anonymity was originally introduced in the context of relational data privacy [25,23]. The k-anonymity model with respect to location information was defined as follows: A query message from a user to a server is called k-anonymous in location-based services if the user cannot be identified by the server based on the user location from the other $k - 1$ users where k is a user-specified anonymity set size [7].

A trusted third party called anonymizer is basically required to achieve k-anonymity with respect to location information since it is hard to construct a cloaked region including k users' queries in a distributed manner [28]. In order to provide k-anonymity, many techniques [12,18,3,10] were proposed based on the assumption of a trusted anonymizer. Fig. 2 illustrates a three-tier architecture with a trusted anonymizer. All queries and answers are relayed through the anonymizer. Given a query, the anonymizer removes the user's identifier, applies cloaking to replace the user location with a cloaked region, and then forwards the cloaked region to the location server.

However, in real applications, the assumption of a trusted anonymizer is not desirable. First of all, we should consider major redesign of technologies (e.g., protocols or trusted mechanism) or business models. It may be not easy to share private service information including map or POIs with other business entities including the anonymizer since the information in location-based services is generally valuable. Second, we should consider the problems inherent in a

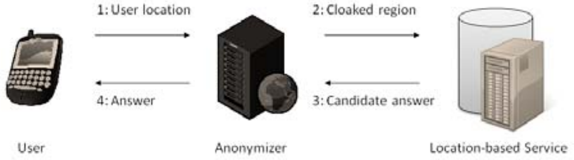


Fig. 2. Three-tier architecture with a trusted third party

single server design since query and response process should always be processed through trusted third party. Moreover, the anonymizer is a single point of attack: if an adversary gains access to it, the privacy of all users is compromised. Third, a large number of users must subscribe to the service, otherwise the cloaked region may not be constructed. It is also assumed that all users are trustworthy. If some of them are compromised, the privacy of a targeted user may be threatened.

In order to overcome the limitation of three-tier architecture, several research efforts are dedicated to constructing a cloaked region at the user (e.g., false dummies [14], landmark objects [11], location perturbation [5,28], transformation-based matching using an obfuscated map [13,16] and transformation-based matching using Private Information Retrieval (PIR) [9]). In the spatial cloaking using dummies, however, the adversary approximately estimates the user location with high accuracy by using cellular positionning techniques [22] or target tracking. In the cloaked region using landmark objects, the accuracy of the answer cannot be generally guaranteed. Transformation-based matching using an obfuscated map also requires a trusted entity that creates an obfuscated map. Transformation-based matching using PIR theoretically provides high privacy but it incurs significant communication and computational overheads compared to other solutions [8].

SpaceTwist [28] incrementally updated the candidate answer without the fixed cloaked region using a faked location called anchor location which is initially set to a location randomly generated by the user. However it consists of multiple message rounds, which may lead to increased response time. Moreover, it cannot always guarantee the user's desired level of privacy.

3 Preliminaries

In this section, we first introduce Voronoi diagram, which is used as a basic data structure in the proposed framework and then define the notations, and threat model.

3.1 Voronoi Diagram

Let $P = \{p_1, p_2, \cdots, p_n\}$ be a set of n points (called sites) in the multi-dimensional Euclidean space. We define the Voronoi diagram of P as the subdivision of the space into n cells, one for each site in P, with the property that a point q lies in the cell corresponding a site p_i if and only if the $dist(q, p_i) < dist(q, p_j)$ for each $p_j \in P$ with $j \neq i$ where $dist$ denotes the euclidean distance function.

We denote the Voronoi diagram of P by $Vor(P)$. The cell of $Vor(P)$ that corresponds to a site p_i is denoted $V(p_i)$; we call it the Voronoi cell of p_i [4].

3.2 Notations

The symbols U and L represent a user and a location server, respectively. The symbol q represents a query position and N a set of the nearest neighbors. The subscript X in N_X implies that a POI in N_X is the nearest neighbor from any point within the region X. A is a function to compute a cloaked region with q and s where q is randomly located on the region $A(q, s)$ and s is a security parameter which is relevant to the level of privacy. For example, $A(q, s)$ is a disc with the radius of s. $D(P)$ is a function to compute the smallest enclosing disc for a set of points P.

3.3 Threat Model

In our model, the adversary is attempting to infer user location by monitoring the communication between a user and a service. Each user has its own privacy requirement A_{min} that specifies its desired level of privacy. A_{min} specifies the minimum resolution of the cloaked spatial region. Our goal is to protect the information about user location so that the adversary only knows the region A in which the user is located, but not her exact location in A where the size of A is greater than A_{min}.

4 The Proposed Framework

The proposed framework is basically based on processing of range search query.

4.1 Protocol

The protocol between U and L is briefly described in Algorithm 1. The cloaked region $A(q, s)$ is generally regarded as a convex polygon with m vertices. $A(q, s)$ can be simply computed as a disc with the radius of s where s is the half of the diameter of A_{min}. The proposed protocol results in $O(k \cdot l_1 + m \cdot l_2)$ bits of communication where k is the number of Voronoi cells which intersect with $A(q, s)$ and l_1 and l_2 are the minimum bits to encode a point and a vertex of a polygon, respectively. L can compute $N_{A(q,s)}$ using the Voronoi diagram for POIs. Finally, after receiving the query response $N_{A(q,s)}$, U can find the nearest POI N_q, by filtering out the false positives from $N_{A(q,s)}$ since $N_{A(q,s)}$ contains N_q. U's computational cost depends on the data structure for representing $N_{A(q,s)}$. The nearest POI N_q from U's location q can be computed in $O(\log k)$ time by locating the cell of Voronoi diagram that contains q when the query response is delivered as the Voronoi diagram $Vor(N_{A(q,s)})$.

Algorithm 1. Spatial cloaking protocol

```
U: Generate $A(q,s)$ including $q$ randomly where the size of $A(q,s)$ is greater than $A_{min}$.
U: Send $A(q,s)$ to $L$.
L: Compute a set of the nearest neighbors $N_{A(q,s)}$ for $A(q,s)$ where $N_{A(q,s)}$ is the set of POIs on the Voronoi cells which intersects with $A(q,s)$.
L: Send $N_{A(q,s)}$ to $U$.
U: Retrieve the nearest site $N_q$ to $q$ from $N_{A(q,s)}$.
```

4.2 Query Processing

The query processing is based on computation of Voronoi diagram for POIs. We formally define the problem as follows: Given a set $S \overset{def}{\equiv} \{p_1, p_2, ..., p_n\}$ of n distinct points in R^2 and a convex polygon P with m vertices, find a set of the nearest neighbors N_P for P.

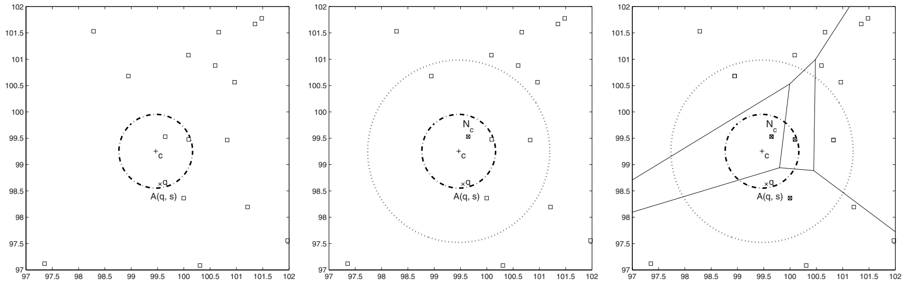
We propose the query processing algorithm using a local Voronoi diagram relevant to the cloaked region since itt is not efficient to maintain the Voronoi diagram for a large entire data set. In particular, for dynamic POIs, the concept of a local Voronoi diagram relevant to the cloaked region is necessarily required since the pre-processed Voronoi diagram is useless when the locations of POIs are dynamically changed. The procedure to compute the intersected Voronoi cells with a polygon P is designed in Algorithm 2.

Algorithm 2. Query processing algorithm

```
Input: a set $S$ of $n$ points, a convex polygon $P$
Output: $N_P$
Find the smallest enclosing disc $D(P)$ for the convex polygon $P$. Let $r$ and $c$ be the radius and the center of $D(P)$, respectively.
Initialize $d$ as $\infty$.
for $s_i \in S$ do
    if $d > dist(c, s_i)$ then
        $d = dist(c, s_i)$
    end if
end for
$r^* = 2 \cdot r + d$
for $s_i \in S$ do
    if $r^* \geq dist(c, s_i)$ then
        Insert $s_i$ into the set of candidate points $S_P$.
    end if
end for
Compute the Voronoi diagram $Vor(S_P)$ for $S_P$.
for $s_i \in S_P$ do
    if a cell $V(s_i) \in Vor(S_P)$ intersects with $P$ then
        Insert $s_i$ into $N_P$.
    end if
end for
return $N_P$
```

Our goal is to identify the minimum set of POIs including the nearest neighbor to the user location. For simple calculation of a threshold r^* for candidate POIs, we use the smallest enclosing disc $D(P)$. The maximum distance d between the enclosing disc $D(P)$ and the nearest POI to the center of $D(P)$ can be used for computing a threshold r^* to choose an adequate set of candidate POIs.

Fig. 3 exemplifies Algorithm 2. Given the user location q and the security parameter s, U constructs a circular cloaked region $A(q, s)$ as the query input (see Figure 2a). L finds a set of candidate POIs for $A(q, s)$ (see Figure 2b) and then compute the local Voronoi diagram for the set (see Figure 2c). Finally, the information about three intersected Voronoi cells with $A(q, s)$ is answered as the query response.



(a) A cloaked region (b) Finding candidate POIs (c) Finding intersections

Fig. 3. A query processing example

Theorem. 1 states that Algorithm 2 is correctly terminated.

Theorem 1. *In Algorithm 2, the nearest POI N_q of the query position q is necessarily included in N_P.*

Proof. Assume that N_q is not included in N_P. From the assumption, the distance between N_q and the center c of $D(V_P)$ is more than $2 \cdot r + d$. Let N_c be the nearest POI from c. The maximum distance between the enclosing disc $D(P)$ and N_c is $r + d$. Let f be the farthest point on $D(P)$ from N_c.

$$dist(q, N_c) \leq dist(f, N_c) \leq r + d < dist(q, N_q)$$

Therefore N_q is not the nearest POI from q. This result contradicts the assumption.

By Theorem. 1, we can intuitively design the $(r + d)$-approximate algorithm with $O(1)$ communication cost. The nearest POI N_c from the center c is an approximation to the given cloaked region $A(q, s)$.

Theorem 2. *Algorithm 2 runs in $O(n + t \log t + m)$ time where t is the number of POIs $\in S_P$.*

Proof. We show that Algorithm 2 runs in $O(n + t \log t + m)$ time by analysing the time needed in each step. We start by finding the smallest enclosing disc $D(P)$ for P with m vertices in line 1 which can be solved in $O(m)$ time [17]. Finding the nearest POI N_c from the center c of $D(P)$ in line 3-7 can be solved in $O(n)$ time. Similarly, finding S_P in line 9-13 can be solved in $O(n)$ time. Computing the Voronoi diagram, $Vor(S_P)$, for S_P in line 14 can be solved in $O(t \log t)$ time [24,21,15]. Finding the intersected Voronoi cells with P in line 15-20 can be computed in $O(t + m)$ time [27]. Consequently, the total running time is in $O(n + t \log t + m)$.

The running time of the Algorithm 2 can be improved by using pre-processed data-structures. Finding the nearest POI N_c from the center c of $D(P)$ in line 3-7 can be improved in $O(\log n)$ time. Also, finding S_P in line 9-13 can be improved in $O(\log n + t)$ [2]. In this case, the total running time is in $O(\log n + t \log t + m)$.

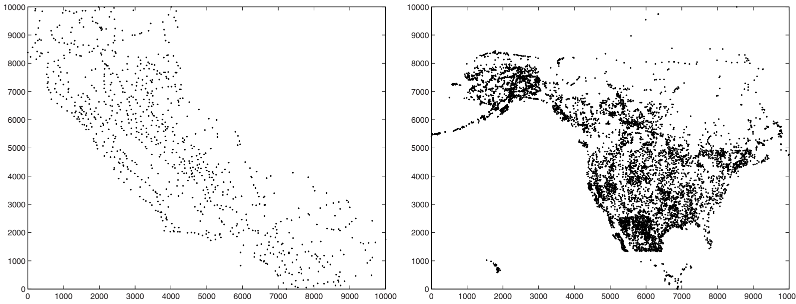
4.3 Approximation Using Sampling

For exact nearest neighbor search, any spatial cloaking techniques including ours may be infeasible depending on scenarios that require extremely high privacy since a larger cloaked region necessarily incurs high communication cost. Considering the constraint of communication cost, the problem can be redefined as follows: Given a constant k_{max}, find a query response with the size which is less than k_{max} for nearest neighbor search. Unfortunately, to achieve this, it is unavoidable to deteriorate accuracy of answer when k_{max} is less than the number of the Voronoi cells which intersect with the cloaked region.

Our strategy is to retrieve POIs according to likelihood. Since the query point q is randomly located at $A(q, s)$, the associated Voronoi cells intersecting the cloaked region $A(q, s)$ as large as possible may be reasonable candidates. This greedy approach guarantees the maximum hit probability of N_q. In Algorithm 2, L computes the size of the intersected area of each Voronoi cell, respectively, and then sorts them in descending order. The first associated k_{max} POIs are answered as the approximate query response. Experimental results have been shown to perform well in practice.

5 Evaluation

In this section, we experimentally evaluate location server L's computational cost, the communication cost and the error distance. The computational cost is measured in terms of the number of POIs computed for the local Voronoi diagram. The communication cost is measured in terms of the number of TCP/IP packets to deliver candidate POIs sent from L back to the user U. We assume that the packet capacity is set to (576-40)/8=67 since a 2D data point takes 8 bytes, a packet has a 40-byte header, and the typical value of a maximum transmission unit (MTU) over a network is 576 bytes [28]. The result error distance is defined as the distance to the candidate nearest neighbor in the query response minus the distance to the actual nearest neighbor.



(a) CA data set

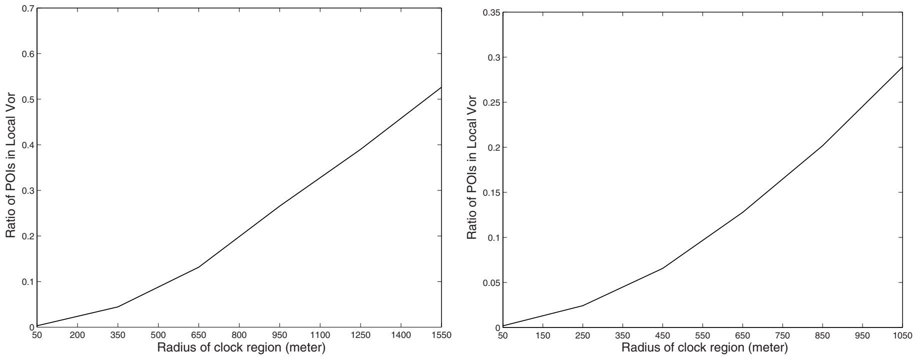
(b) NA data set

Fig. 4. Two data sets

We use the two real datasets: California (CA) with 864 POIs and North-America (NA) with 9,203 POIs (Fig. 4) [26]. The coordinates of points in each dataset are normalized to the square 2D space with extent 10,000 meters. We test the performance by varying the radii of cloaked regions from 50 to 1,550 meters for the CA (from 50 to 1,050 meters for the NA). We generated 100 queries originating at random positions using the Gaussian distribution of the POIs in each dataset.

Regarding the server L's computational cost, we measure the ratio of the POIs that are used to compute the local Voronoi diagram to the entire POIs in each dataset. Fig. 5 shows the relationship between the size of a cloaked region and the number of POIs in a local Voronoi diagram.

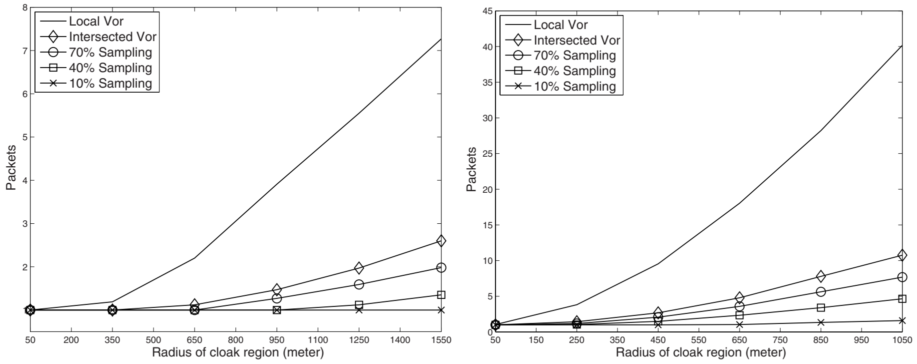
Fig. 6 shows the experimental results for the communication cost. In order to evaluate the performance of our framework, we compare it with a basic spatial cloaking approach (Local Vor in Fig. 6) where all POIs in S_P for local Voronoi diagrams are answered as the query response for nearest neighbor search. For larger cloaked regions, the communication cost of the basic spatial cloaking is



(a) CA

(b) NA

Fig. 5. Size of local Voronoi diagram



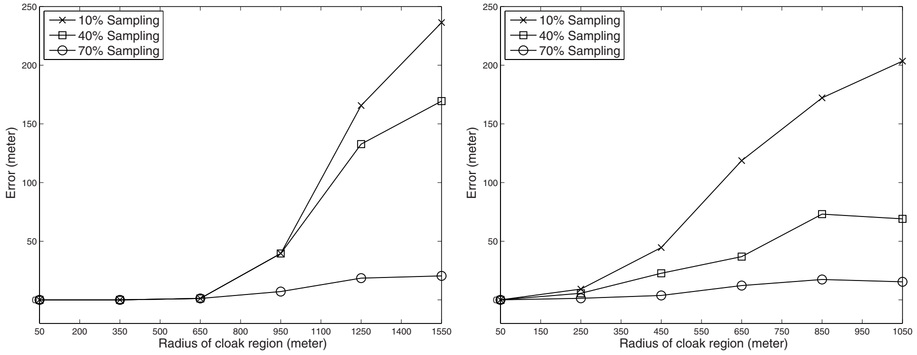
(a) CA

(b) NA

Fig. 6. Communication cost

dramatically increasing while the proposed scheme based on the intersected Voronoi cells (Intersected Vor in Fig. 6) is practically acceptable. For example, in CA dataset with sparse POIs, the total communication cost of the proposed scheme is bounded by 3 packets even if the radius of a cloaked region is 1,550 meters.

Fig. 7 shows the measured error distance in sampling methods. Not surprisingly, the communication cost and the result error increases with the size of the cloaked region, respectively. Experimental results show how the proportion of sampling can be set depending on the level of privacy and the communication constraint. In the proposed scheme, a user can achieve the maximum permitted communication cost by controlling the proportion of sampling from intersected Voronoi cells. In these datasets, the sampling of 70% intersected Voronoi cells scales well with the size of the cloaked region. We observe that the sampling method based on Voronoi diagram offer reasonable accuracy and low communication cost.



(a) CA

(b) NA

Fig. 7. Distance error

The proposed scheme guarantees that the adversary cannot obtain the information about user location within the cloaked region. The security requirement is achieved defined in Section 3.3 since the size of the cloaked region is greater than A_{min} by the proposed protocol.

6 Conclusions

In this paper, we proposed a spatial cloaking using range search in location-based services for nearest neighbor search. The main idea is to use the adaptive range search query based on Voronoi diagram. In our model, the spatial cloaking problem is interpreted as finding the intersections of Voronoi cells with a cloaked region. We propose a simpler and more flexible protocol based on computation of the Voronoi diagram which we are locally interested. Also, we experimentally investigate the trade-offs between communication/computational cost and levels of privacy (sizes of cloaked regions). Therefore it is applicable in simple client-server architectures since our architecture does not require a trusted middleware. Also, users can flexibly achieve the required communication cost by controlling the proportion of sampling from intersected Voronoi cells.

We will study the extension of the proposed system using the network Voronoi diagram [20] to the road networks with the movement on line segments instead of free-moving since the user's available movement may be restricted by paths such as roads in real applications. Also, one of interesting applications is optimal route planning problem [19,6].

Acknowledgements

The author would like to thank Ross Anderson, Alastair Beresford, and Ji Won Yoon for their careful attention and insightful comments.

References

1. Google latitude (2009)
2. Aggarwal, A., Hansen, M., Leighton, T.: Solving query-retrieval problems by compacting voronoi diagrams. In: STOC 1990: Proceedings of the twenty-second annual ACM symposium on Theory of computing, pp. 331–340. ACM, New York (1990)
3. Chow, C.-Y., Mokbel, M.: Enabling private continuous queries for revealed user locations, pp. 258–275 (2007)
4. de Berg, M., Cheong, O., van Kreveld, M., Overmars, M.: Computational Geometry: Algorithms and Applications, 3rd edn. Springer, Berlin
5. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Gellersen, H.-W., Want, R., Schmidt, A. (eds.) PERVASIVE 2005. LNCS, vol. 3468, pp. 152–170. Springer, Heidelberg (2005)
6. Frikken, K.B., Atallah, M.J.: Privacy preserving route planning. In: WPES 2004: Proceedings of the 2004 ACM workshop on Privacy in the electronic society, pp. 8–15. ACM, New York (2004)

7. Gedik, B., Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing 7(1), 1–18 (2008)
8. Ghinita, G.: Understanding the privacy-efficiency trade-off in location based queries. In: SPRINGL 2008: Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, pp. 1–5. ACM, New York (2008)
9. Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., Tan, K.-L.: Private queries in location based services: anonymizers are not necessary. In: SIGMOD 2008: Proceedings of the 2008 ACM SIGMOD international conference on Management of data, pp. 121–132. ACM, New York (2008)
10. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: MobiSys 2003: Proceedings of the 1st international conference on Mobile systems, applications and services, pp. 31–42. ACM, New York (2003)
11. Hong, J.I., Landay, J.A.: An architecture for privacy-sensitive ubiquitous computing. In: MobiSys 2004: Proceedings of the 2nd international conference on Mobile systems, applications, and services, pp. 177–189. ACM, New York (2004)
12. Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing location-based identity inference in anonymous spatial queries. IEEE Transactions on Knowledge and Data Engineering 19(12), 1719–1733 (2007)
13. Khoshgozaran, A., Shahabi, C.: Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In: Papadias, D., Zhang, D., Kollios, G. (eds.) SSTD 2007. LNCS, vol. 4605, pp. 239–257. Springer, Heidelberg (2007)
14. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings. International Conference on Pervasive Services, ICPS 2005, July 2005, pp. 88–97 (2005)
15. Lee, D.: Furthest neighbour voronoi diagrams and applications. Technical Report Report 80-11-FC-04, Dept. Elect. Engrg. Comput. Sci., Northwestern Univ., Evanston, IL (1980)
16. Maria Damiani, C.S.: Elisa Bertino. Probe: an obfuscation system for the protection of sensitive location information in lbs. Technical report
17. Megiddo, N.: Linear-time algorithms for linear programming in r3 and related problems. In: 23rd Annual Symposium on Foundations of Computer Science, 1982. SFCS 2008, November 1982, pp. 329–338 (1982)
18. Mokbel, M.F., Chow, C.-Y., Aref, W.G.: The new casper: query processing for location services without compromising privacy. In: Proceedings of the 32nd international conference on Very large data bases, pp. 763–774. ACM, New York (2006)
19. Nergiz, M.E., Atzori, M., Saygin, Y.: Towards trajectory anonymization: a generalization-based approach. In: SPRINGL 2008: Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, pp. 52–61. ACM, New York (2008)
20. Okabe, A., Boots, B., Sugihara, K., Chi, S.N.: Spatial Tessellations: Concepts and Applications of Voronoi Diagrams, 2nd edn. Wiley, Chichester (2000)
21. Preparata, F.P.: Minimum spanning circle. Technical report, Univ. Illinois, Urbana, IL, in: Steps into Computational Geometry (1977)
22. Reed, J., Krizman, K., Woerner, B., Rappaport, T.: An overview of the challenges and progress in meeting the e-911 requirement for location service. IEEE Communications Magazine 36(4), 30–37 (1998)

23. Samarati, P., Sweeney, L.: Generalizing data to provide anonymity when disclosing information (abstract). In: PODS 1998: Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, p. 188. ACM, New York (1998)
24. Shamos, M.I., Hoey, D.: Closest-point problems. In: SFCS 1975: Proceedings of the 16th Annual Symposium on Foundations of Computer Science (sfcs 1975), Washington, DC, USA, pp. 151–162. IEEE Computer Society, Los Alamitos (1975)
25. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10(5), 557–570 (2002)
26. Theodoridis, Y.: The r-tree-portal (2009)
27. Toussaint, G.T.: A simple linear algorithm for intersecting convex polygons. The Visual Computer 1, 118–123 (1985)
28. Yiu, M.L., Jensen, C., Huang, X., Lu, H.: Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: IEEE 24th International Conference on Data Engineering, ICDE 2008, April 2008, pp. 366–375 (2008)