International Journal of Innovative Computing, Information and Control
Volume **13**, Number **2**, April **2017**

ICIC International ©2017 ISSN 1349-4198
pp. 441–452

A FAST PRIVACY-PRESERVING CLOAKING ALGORITHM IN ROAD NETWORKS

Xianshan Li[1,2], Xiuxiu Fang[1,2], Maoyuan Sun[1,2], Jiadong Ren[1,2] and Fengda Zhao[1,2,*]

[1]College of Information Science and Engineering
[2]The Key Laboratory for Software Engineering of Hebei Province
Yanshan University
No. 438, West Hebei Ave., Qinhuangdao 066004, P. R. China
{ xjlxs; jdren }@ysu.edu.cn; *Corresponding author: zfd@ysu.edu.cn

Received September 2016; revised January 2017

Abstract. *The location-based services (LBS) bring convenience to people's daily life; however, at the same time it also tends to threaten the privacy of its users, as users have to submit the exact location with a query to the LBS. To address this issue, spatial anonymity technique is used to expand users' exact location and then send the position to the LBS. In this paper, we propose a new efficient Hilbert-based cloaking algorithm, called EHilbertCloak, to protect personal privacy. First of all, our algorithm guarantees K-anonymity under the strict reciprocity condition. Secondly, the EHilbertCloak algorithm uses anonymous processing of multiple users at the same time to improve the efficiency of anonymity. To guarantee the quality of service, the total length of the anonymous region cannot exceed a certain distance limit. So we only consider these edges with active users. Thirdly, our algorithm increases the anonymous success rate by adding dummy users in anonymous region. Finally, an extensive experimental study in real road networks shows that the proposed algorithm outperforms the state-of-the-art algorithm for the task.*
Keywords: LBS, Hilbert-order, K-anonymity, Cloaking algorithm, Reciprocity condition

1. **Introduction.** Location-based services (LBS) are emerging as a major application of mobile geospatial technologies [1-4]. In LBS, users with location-aware mobile devices are able to make queries about their surroundings at anywhere and anytime (e.g., "show me the nearest hotels to my current location"). In order to get the precise answers of these queries, users have to disclose their exact position information to the LBS. However, in this process the user's private information may be revealed or misused [5]. An adversary can get the user's location information through different ways. Therefore, the location information as the foundation for LBSs has profound implications on the personal privacy. Today people are increasingly aware of privacy issues and reluctant to expose their personal information [6].

A lot of research has been conducted concerning how to enjoy location-based services and protect the location privacy of mobile users [7-11]. These anonymity techniques obfuscate user locations, making it difficult to distinguish a user from others. Even if the attacker knows the exact location information of user within the anonymous region, he cannot determine the querying user and the probability of user being attacked is $1/K$. However, most of the existing location privacy protection methods were based on the Euclidean space [1-3,5-11]. In Euclidean space, the moving direction of the user is arbitrary without any restrictions. However, in real life, the user's driving direction is subject to certain restrictions such as traveling along a certain road or traveling in

limited speed. Therefore, we put forward the location privacy protection method based on the road network condition. Palanisamy and Liu [12] proposed a suite of road network mix-zone construction. However, it pays no consideration to the network updating, which may lead to system unavailability in the long run. Inspired by the mix-zone concept, Meyerowitz and Choudhury [13] proposed CacheCloak, which exploits cache prefetching to prevent query tracking attacks. Bao et al. [14] proposed a peer-to-peer location privacy-preserving system called pros, in which a user collaborates with others to form a cloaked road segment set. Cho et al. [15] proposed a privacy-aware monitoring algorithm for preserving the trajectory privacy of MkkNN queries in road networks. Wang and Liu [16] proposed X-Star subgraph anonymous model whose basic idea is to convert road network graph into sub graph of star graph, and the degree of nodes is not less than three. Although X-Star can meet reciprocity condition, the total length of the anonymous region easily exceeds a certain distance limit; thus it increases the cost of query processing. Kim et al. [17] improved the X-star algorithm combined with Hilbert curve and proposed an H-star algorithm. The H-star algorithms based on Hilbert curve ordered the star nodes, and loaded them into the bucket according to anonymity degree K. Although this algorithm had some improvements, it suffers from the same problem as the X-star. Li and Palanisamy [18] proposed a new class of reversible location cloaking mechanisms that effectively support multi-level location privacy. Ma and Zhou [19] proposed a Voronoi-based network diagram which is based on partitioning a large network to small Voronoi regions. It precomputed intermediate results in memory and constructs query answers based on the caches results. Wang and Xia [20] proposed an Snet hierarchy structure for a single user and a batch of users. Each Snet is treated as a cloaking unit. Although Snet hierarchy structure can accelerate the privacy-preserving process, the Snet hierarchy cannot be updated in time; thus it reduces the anonymous success rate. Kalnis et al. [21] proposed a location cloaking algorithm called Hilbert Cloak, in which all user locations were sorted and grouped by Hilbert space-filling curve ordering. Since our idea is derived from the Hilbert Cloak [21], the Hilbert Cloak algorithm will be described in more detail.

Hilbert Cloak satisfies Reciprocity Condition which is an important property for spatial K-anonymity. The Hilbert space-filling curve transforms the 2D coordinates of each node into a 1D value. Figure 1 illustrates the Hilbert curves for a 2D space by using a $4*4$ space partitioning. With high probability, if two points are in close proximity in the 2D space, they will also be close in the 1D transformation. A major benefit of Hilbert curves is that they permit the indexing of multidimensional objects through 1D structure (for example, B-trees). Hilbert Cloak splits the user into K-bucket; each K-bucket has at least k users, except for the last one, which may contain up to $2K - 1$ users. Hilbert Cloak algorithm

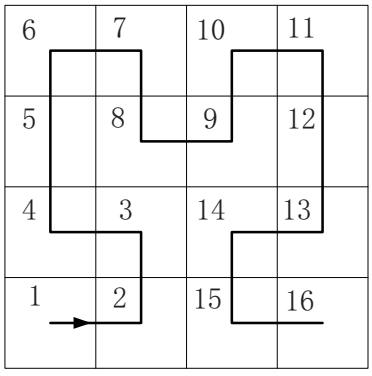

FIGURE 1. Hilbert curve $4 * 4$

is the only proven secure algorithm, and has been applied in P2P systems. Therefore, we apply this algorithm to the road network environment.

Currently, several privacy-preserving solutions have been introduced to road networks [16,17,19]. Unfortunately, existing approaches (including the Hilbert Cloak algorithm [21] described above) show poor successful anonymization rate and huge anonymity time. To avoid such huge time cost and poor successful rate in the traditional approaches, we propose a new efficient Hilbert-based cloaking algorithm, called EHilbertCloak, which improves anonymous success rate and decrease anonymity time cost. This cloaking algorithm performs faster to process a batch of user simultaneously instead of processing a single user at one time. Furthermore, we consider sparsely populated areas are difficult to find k users. So the cloaking adds the dummy user in the cloaked region. The contributions of this paper can be summarized as follows.

- We propose a K-anonymity based cloaking framework where an anonymous region is generated based on the anonymity degree K of querying user and it expands the anonymous region until it fulfills user's requirement.
- We improve the speed of user's anonymity by using anonymous processing of multiple users at the same time and avoid such high anonymity time cost in the traditional approaches. Since the anonymity set is to meet the conditions of reciprocity, users in the anonymizing set can concentrate anonymous only once.
- We propose a method to generate a dummy user in anonymous region. Because in sparsely populated region or when anonymity degree K is too high, it is hard to find the k users within a certain range which caused the low anonymous success rate. Although this method generates the anonymous region is less than k real users, the probability of querying user being attacked is still less than $1/K$.

In this paper, we only consider the edge that has active users. The system is composed of a trusted third party acting as a middle layer between mobile users and LBS providers. When a user sends queries to trusted third party, K-anonymity for each query can be guaranteed [6].

The rest of our paper is organized as follows. We present the system model and privacy metrics in Section 2. A new efficient cloaking algorithm called EHilbertCloak is proposed in Section 3. Section 4 presents the performance evaluation results of our proposed algorithm, and conclusions are drawn in Section 5.

2. System Model and Privacy Metrics.

In this section, we formally define the problem under study. Section 2.1 describes the system architecture. Section 2.2 depicts the road network. The privacy model is defined in Section 2.3.

2.1. System architecture.

We propose an anonymous query processing framework targeted at road network databases. We adopt the trusted anonymizer (AZ) model (i.e., the use of the AZ as a mediator between users and the LBS) as illustrated in Figure 2. A mobile user sends location-based query requests (e.g., "finding the nearest hospital") in the form of $\langle u, l, p, q\rangle$ to the AZ through an authenticated and encrypted connection where u is the identifier of the user, l is the user's current location, p contains the privacy parameters (to be detailed in Section 2.3), and q is the query text.

When users log on to the system, it establishes a secure connection with the AZ. Through this connection, they update their locations to the AZ. When a user makes a query, first, the AZ is responsible for receiving the query and the exact position information from the mobile user. Second, the AZ generates anonymous region R according to the user's privacy requirements and relays it to the LBS server. Third, the service provider receives a location based query request; they will search and return all candidate

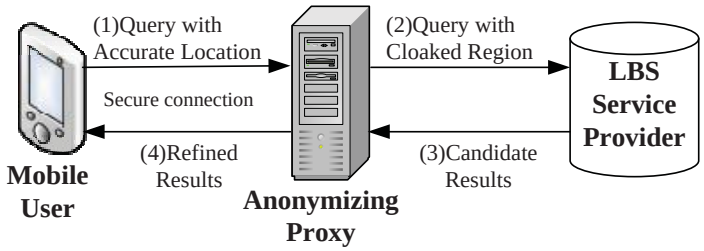

FIGURE 2. The system architecture

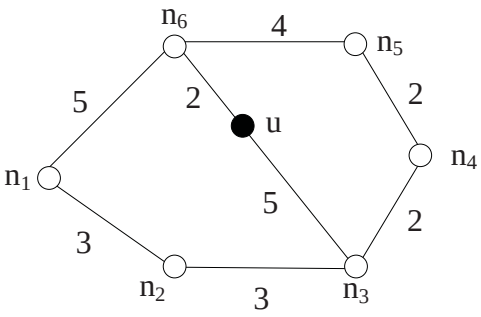

FIGURE 3. Road network

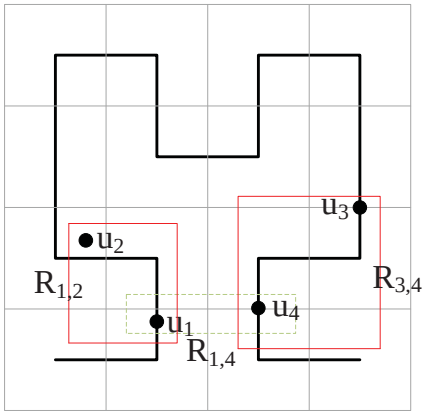

FIGURE 4. Hilbert cloak

results which are potentially query results of some location point. Finally, the AZ filters out these candidate results by the user's exact location l and sends the exact answer to the mobile users.

2.2. **The road network.** We consider a space which is restricted by the underlying road network. The road network is represented by a weighted directed graph $G = (N, E)$, where N is the set of network nodes, and E the set of edges. Every edge e in E connects two nodes and is associated with a nonnegative weight $w(e)$. Weight $w(e)$ may represent the traveling time from one node to the other or the length of the road. In this paper, weight $w(e)$ represents the latter. An example of the road network model is shown in Figure 3. Edge n_1n_2 has weight 3, and its endpoints are nodes n_1 and n_2. When no confusion occurs and to simplify, we do not explicitly mention the directions of the underlying road network in figures appearing in subsequent sections. In all our illustrations, we apply user locations to solid points, the edge of the endpoint as hollow points.

We arrange the edge midpoints by using Hilbert order as shown in Figure 1. The Hilbert values of the edge midpoints are used as their sorting keys. To map user coordinates to their containing edge, these edges are indexed by a PMR quadtree [22]. In particular, if the edge of user u has smaller order than that of u_0, a user u precedes u_0. If u and u_0 fall on the same edge n_in_j and u closer to n_i, u precedes u_0. This precedence relationship defines the user's order. The number on each edge indicates edge's order and the user's subscript represents user's order. Figure 5 shows a road network and an ordering of its edges. The number 3 on the edge n_2n_{14} is the order of the edge. There are two users on the edge n_2n_{14} and u_3 is closer to the n_2 than u_4. So the order of u_3 is less than u_4. The edges corresponding to the bucket of the querying user u are called the anonymizing edge list (AEL) of u.

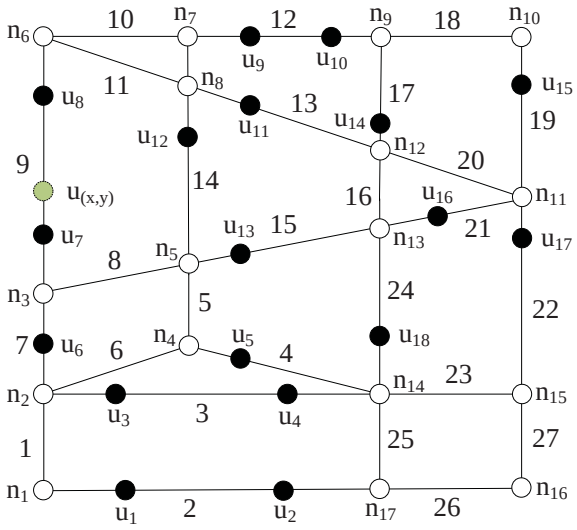

FIGURE 5. Ordering road network

2.3. **Privacy metrics.**

Definition 2.1. $(K; L\max; T\max)$. *In order to accommodate personalized privacy requirements, each user can specify three parameters for protecting the location privacy.*

- K*: It represents the anonymity level in the location* K *anonymity model. In other words, each anonymous region should cover at least* k *different users. With the value of* K *becoming larger, more privacy is offered.*
- $L\max$*: It specifies the maximum length of the anonymizing edge list (AEL). It prevents the anonymizing edge list from being too large for sparsely populated areas.*
- $T\max$*: The longest anonymous time from the user putting forward query to the end of anonymity which users can tolerate. If the time of anonymity proceeding is more than* $T\max$*, query fails.*

The AZ anonymizes u with a set of line segments/edges instead of a spatial region. It is noted that the minimum length of AEL could also be used as a QoS parameter. Nevertheless, to simplify our privacy model, we do not require limiting the minimum length of AEL.

Definition 2.2. *The reciprocity condition: The original definition [7] states that an AEL satisfies the reciprocity condition if a) it contains the requester and at least* $k-1$ *additional users and b) each AEL must be shared by at least* k *users.*

It is worth noting that to ensure effective defending of Hilbert Cloak against the query sampling attack, every K-anonymous region is required to satisfy the reciprocity condition. As shown in Figure 4, users u_1 and u_2 share the same 2-anonymous region $R_{1,2}$, and users u_3 and u_4 share the same 2-anonymous region $R_{3,4}$. In this way, the adversary cannot infer who between them posed a query with ASR $R_{1,2}$. In contrast, users u_1 and u_4 share the same 2-anonymous region $R_{3,4}$, u_2 has the 2-anonymous region $R_{1,2}$, and u_3 has the 2-anonymous region $R_{3,4}$. In this way, the adversary can infer u_2 posed a query with ASR $R_{1,2}$ and u_3 posed a query with ASR $R_{3,4}$.

Definition 2.3. *Dummy user: In AEL randomly generate geographic coordinates* (x, y) *as the dummy user's coordinates. The location privacy protection parameter of the dummy user is the same as the privacy parameter of the real user.*

TABLE 1. Interpretation of acronyms and symbols

AZ	Anonymizer
LBS	Location-based services
AEL	Anonymizing edge list
AS	Anonymizing set
K	Anonymity degree K
L max	the maximum length of AEL

To conclude this section, we list the interpretation of primary symbols and acronyms in Table 1 used throughout the paper.

3. **Hilbert-Order Based Cloaking Algorithm.** In this section, we first give the overview of EHilbertCloak algorithm in Section 3.1. In Section 3.2, we present an algorithm to improve the efficiency of road privacy preserving framework. It generates *AEL* for a batch of users to reduce the cloaking time. We put forward an algorithm for generating dummy users in Section 3.3.

3.1. **Overview of EHilbertCloak algorithm.** Note that the users mentioned in the text are already registered users and AZ can get the user's location. When a user u poses a query requiring anonymity degree K, the first task of the AZ is to acquire the user's order $ordu$ and the order $orde$ of edge where this user exists. According to the $ordu$ and anonymity degree K, we can determine the order interval of K users in the K-bucket. The formulas of calculating the min order and max order are as follows.

$$\min\_ord = ordu - (ordu - 1) \bmod K \tag{1}$$

$$\max\_ord = \min\_ord + K - 1 \tag{2}$$

The AZ extends edge $orde$ to its two sides, until the user's order is less than the $\min\_ord$ on the one side, and the user's order is greater than the $\max\_ord$ on the other side. AZ can find k users and put them into AS. Finally, AZ forms the AEL by collecting corresponding edges to AS of the querying user u. AZ will skip this edge when there is no user in the process of extending. If we put no users' edges into AEL, the total length of anonymity region is too long which can affect the quality of service. Moreover, the total length of edges in the AEL has a maximum distance limit. Exceeding the maximum will cause the query to fail.

Considering the network shown in Figure 5, it contains 18 users and 27 edges with subscripts indicating their orders respectively (i.e., user u_3 has order 3, and edge e_3 has order 3, etc.). Assume that u_8 poses a query with anonymity degree $K = 5$. Putting u_8 into Formula (1) and Formula (2), AZ can figure out that $\min\_ord = 6$ and $\max\_ord = 10$. User u_8 belongs to e_9. The e_9 has two users u_7 and u_8. So $ASu_8 = \{u_7, u_8\}$ and $AEL = \{e_9\}$. Because u_7 is greater than $\min\_ord$, this algorithm can extend e_9 to the direction of small order. There is no user on e_8, so it skips this edge and continues to extend edge to the direction of small order until the user order is less than $\min\_ord$. It extends this edge to the direction of edge's larger order in the same way. Finally, $ASu_8 = \{u_6, u_7, u_8, u_9, u_{10}\}$ and $AELu_8 = \{e_7, e_9, e_{12}\}$.

In the process of expansion, if the length of the e_i is too long, AZ will skip this edge and continue to extend down. In the above example u_8 has $L\max = 200$, when extended to e_7, $L(AEL(e_9, e_7)) > L\max$, then skip e_7. Finally, $ASu_8 = \{u_7, u_8, u_9, u_{10}\}$ and $AELu_8 = \{e_9, e_{12}\}$. It is easy to see $|ASu_8| < K$, thus generating a dummy user in the

$AELu_8$. As shown in Figure 5 the green solid point represents the dummy user $u_{(x,y)}$. Finally $ASu_8 = \{u_{(x,y)}, u_7, u_8, u_9, u_{10}\}$ and $AELu_8 = \{e_9, e_{12}\}$.

EHilbertCloak algorithm satisfies the reciprocity condition; at the same time, if the users in the same AS are proposed for the query with the same anonymity degree K, the two users have the same AEL. Therefore, the EHilbertCloak algorithm proposes batch processing queries for the same anonymity degree K users. If these users are in the same AS, our algorithm finds anonymity region for only one of them, the rest of the users share this AEL. For example, u_9 and u_8 (above mentioned) propose a query requiring $K = 5$ at the same time. Since they are in the same AS and have the same anonymity degree K, $ASu_9 = \{u_{(x,y)}, u_7, u_8, u_9, u_{10}\}$ and $AELu_9 = \{e_9, e_{12}\}$.

3.2. **EHilbertCloak cloaking algorithm.** As multiple queries may arrive at the AZ simultaneously, the proposed EHilbertCloak generates AEL for a batch of users at one time. In our system, the AS and AEL are shared by all the querying users which are in the same AS.

Algorithm 1: EHilbertCloak cloaking algorithm

Inputs: Query set $\mathrm{q}\langle u, l, k, L\max, T\max\rangle$
Output: Anonymizing set AS, anonymizing edge list AEL
1. map l on edge e; find the order ordu of u and the order of e where u exists
2. $\min\_ord = ordu - (ordu - 1) \bmod K$;
3. $\max\_ord = \min\_ord + K - 1$;
4. $ord\_key = \min\_ord * |U|$
5. **if** exit this ord_key **then**
6. **return** $\mathrm{AS}_{(ord\_key)}$ and $\mathrm{AEL}_{(ord\_key)}$
7. **end if**
8. **while** $|AS| < K$ and $L(\mathrm{AEL}) < L\max$ and $|e_i| > 0$ **do**
9. find the e_i on the left side of the e: the minimum order of users on the e_i is not less than min_ord. AS $\leftarrow u$, AEL $\leftarrow e_i$
10. find the e_i on the right side of the e: the maximum order of users on the e_i is not greater than max_ord. AS $\leftarrow u$, AEL $\leftarrow e_i$
11. **end while**
12. **if** $|AS| <$K
13. generating dummy users
14. **end if**
15. **return** AS and AEL

As is shown in Algorithm 1, user u sends a query in the form of $\langle u, l, k, L\max, T\max\rangle$. When receiving a query q from user u, the AZ maps l into road network. AZ calculates the maximum and minimum order of users in the K-bucket according to the user's ordu (steps 2 and 3). In step 4, $|U|$ represents the number of the querying users and ord_key represents the uniqueness of this [min_ord, max_ord] number range. Then AZ determines whether this interval exists, if exists, return the AS and AEL (steps 4-6). When the AS and $L(AEL)$ meet the user's expansion condition, AZ began to expand the anonymous region of the user (steps 8-11). $|e_i|$ represents the number of users on the edge of e_i. If the number of users in the AS is less than K, then Algorithm 2 is called to generate dummy users (steps 12-14).

3.3. **Generating dummy users.** In densely populated commercial area, it is easy to find k users within a certain range. However, in a sparsely populated area, it can be hard

to find k users, especially when the anonymity degree K is large. If AZ cannot find k users within a certain time range or area, then the user's query fails. So it is necessary to introduce the concept of dummy users. Even if the attacker knows there are dummy users in the region, he cannot know which users are real and which are dummy users, so the probability of the user being attacked is still $1/K$.

Generating the dummy locations totally at random provides little control [23]. We are interested in approaches for generating the dummies that aid in satisfying $\langle k, L\max\rangle$-privacy. We thus propose dummy generation algorithms. All locations, including the user location and the dummy locations, are constrained by Lmax.

Algorithm 2: Generating dummy users algorithm

Inputs: Anonymizing edge list AEL, required anonymity degree K, candidate cloaked set AS
Output: Anonymizing set AS
// f represents the number that needs to generate of dummy users
1. $f = K - |AS|$
2. **for** $i < f$ **do**
3. randomly select e_i in AEL
4. at the e_i generate a random coordinate $(x, y) \rightarrow$ new user $u_{(x,y)}$
5. **if** $u_{(x,y)} \notin$ AS
6. AS $\leftarrow u_{(x,y)}$
7. **end if**
8. **end for**
9. **return** AS

Algorithm 2 will be called when the number of users in AS is less than k. AZ first randomly selected e_i in the AEL, and then randomly selects one point in e_i as the position coordinate of the dummy user (steps 3 and 4). As shown in Figure 5, the green solid point represents the dummy user $u_{(x,y)}$. The location privacy protection parameter of this dummy user is the same as the privacy parameter of the real user.

4. **Experimental Evaluation.** In this section, we evaluate the effectiveness of our proposed algorithm on real road network. Our proposed approach, EHilbertCloak algorithm, has been compared with random edge ordering (RE) and Hilbert-based ordering (HE). The simulating experiments are conducted on a machine with hardware configuration 64 bit Core i5 processors running Ubuntu14.10 and 4GB of free RAM. We implement the algorithms with C++. We randomly generate 60k querying users from 100k users and measure the sum of the anonymous time about them at the AZ. In most of the existing methods, anonymity degree K is a fixed option from several numbers, but each querying user's anonymity degree K can be randomly generated in a certain range in our algorithm.

4.1. **Experiment setup.** We use the real road network of San Francisco, obtained from [24] which originally consisted of 100K mobile users and 50K edges. Weights of the edges are set to their lengths. On this map, we generate 100,000 moving objects. The user locations distribute uniformly. Parameters used in our experiment are listed in Table 2. The values of parameters K and Lmax are selected from the [2-30], 100-700 respectively, and that set of experimental parameters can get better experimental comparison results. For example, for the anonymity degree K, if there is only 1 person in anonymous region, that is the querying user itself, the anonymous query is meaningless. Therefore, the value of K is greater than 2. When K is greater than 30 to get the experimental comparison

TABLE 2. Experiment parameters

Parameters	Values	Default
Number of users	100k	100k
Number of querying users	10k, 20k, 30k, 40k, 50k, 60k	30k
User distribution	Uniform	Uniform
Anonymity degree K	[2,30]	15
Distance limit Lmax	100-700	600

results and $K = 30$ is no different, so we choose the value of K between [2-30]. The default values are used if they are not specifically described in the following experiments. We repeatedly run each experiment for ten times and take the average values as the evaluation results.

4.2. **Evaluation results.** In this section, we illustrate the achieved anonymity and analyze the performance of our algorithm.

Definition 4.1. *Anonymization success rate: it is the rate of the number of success querying users to the total number of querying users. This is a key measure value for quality evaluation of cloaking algorithm:*

$$SR = \frac{|\text{success\_msg}|}{\text{all\_msg}} \tag{3}$$

where all_msg represents all the users of the query message and success_msg means the sum total of the success of the query message. The anonymous time is also the key to evaluation of the algorithm. The following cloaking algorithm time is the sum of the querying user's anonymous time.

The anonymous time is affected by the K value and the number of queries. In general, the larger the anonymous value of K is, or the larger number of users is, the longer anonymous time will be. However, in the EHilbertCloak algorithm, the anonymous time grows slowly and tends to a certain range as shown in Figure 6. This is because it generates the anonymous region for a batch of users. Under the premise of a certain number of querying users, the larger K value becomes, the longer the range of the bucket has, and thus the number of users which are handled at the same time increases. As is shown in Figure 6(a) and Figure 6(c), the anonymous time is not always becoming longer with the K value growing, even it showed a downward trend in Figure 6(c). Under the premise of a certain value of K, the more querying users there are, the bigger probability that users are in the same AS is. Therefore, the number of users which are handled by AZ at the same time is increasing, the anonymous time is not always growing as the number of users increases. Figure 6(a) shows the sum of anonymous time for $50K$ users with these three algorithms. The querying user's anonymity degree K is randomly chosen in a certain range. Figure 6(b) shows the relationship between the number of querying users and the anonymous time when $K = [10, 15]$. When the number of users is small, the three algorithms have little difference in the anonymous time. Comparing Figures 6(a) and 6(c), Figures 6(b) and 6(d), we can see that the anonymous time of EHilbertCloak algorithms increases when K is not equal to a fixed value. For example in Figure 6(b) where K = [10-15], the probability that users have the same K is 1/6. The probability of the user on the same AS is reduced, so the anonymous time increases.

Figure 7 evaluates the success rate influenced by the anonymity degree K and the limit of total length of AEL. It is obvious that EHilbertCloak algorithm can obtain higher success rate under the same anonymity degree K and distance limit. The dummy users

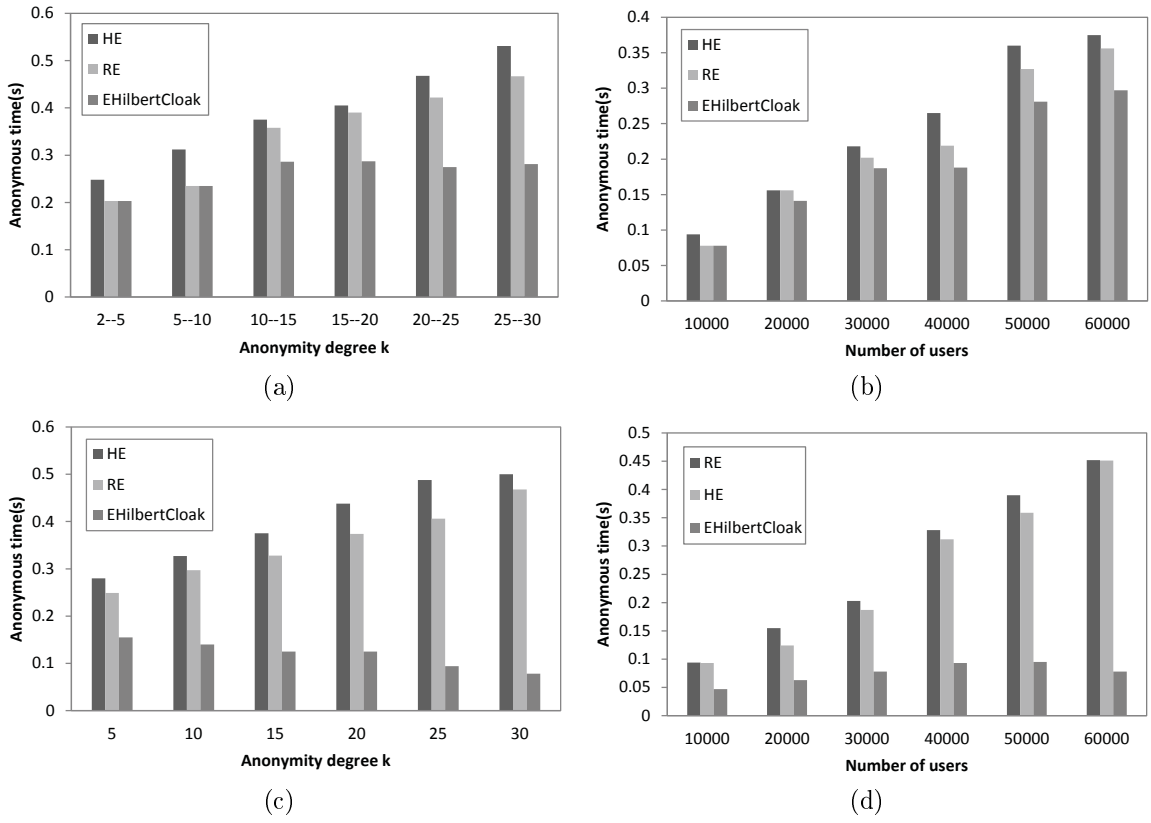

FIGURE 6. Anonymous time evaluation

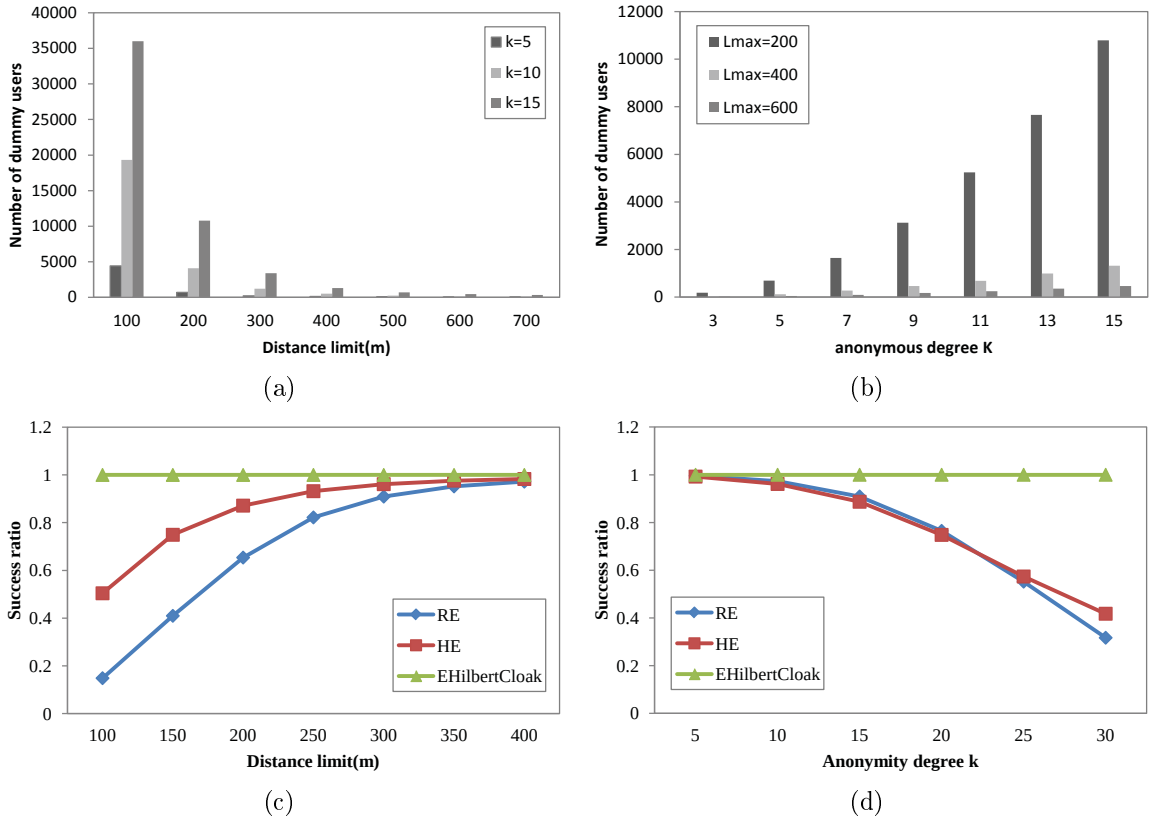

FIGURE 7. Anonymous time evaluation

are generated by 30 thousand queries. Figure 7(a) shows the impact of the number of dummy users with different distance limits in the case of three anonymity degree K. Figure 7(b) exhibits the influence of the number of dummy users with different anonymity degree K in the case of three distance limit. Figure 7(c) shows the influence of the anonymous success rate with distance limit when anonymity degree $K = 15$. In a certain anonymity degree K, with the distance limit becoming larger, we can find k users easier, and therefore the success rate is higher. $L\max = 300$ in Figure 7(d), and it is easier for us to find k users within a certain range with smaller anonymity degree K. So the success rate of the three algorithms is the same value. It is easy to see that the success rate of EHilbertCloak algorithm is the highest among them.

From all the evaluated results, we can conclude that our proposed algorithms can achieve better privacy preservation than RE, HE with the quality of service maintained and success rate improved.

5. **Conclusions.** In this paper, we proposed a EHilbertCloak cloaking algorithm to protect personal privacy in road network. We order the edges of road network by using Hilbert curve to satisfy the reciprocity condition and guarantee K-anonymity. The EHilbertCloak algorithm has four phases: (i) construction of road network model; (ii) mapping edge to Hilbert ID by using Hilbert order; (iii) calculating interval of the K-bucket; (iv) selecting edge expansion phase for fulfilling the user's requirement. Our EHilbertCloak algorithm considers privacy protection in the case of sparse population. An extensive experimental study shows that EHilbertCloak achieves high success rate of anonymization and low communication costs compared with existing HilbertCloak algorithm.

For the next stage of study, we plan more detailed evaluation of our proposal. The simulation evaluation in a realistic mobility model which uses an actual map is also our future tasks. We also plan to investigate the solutions against different classes of attacks.

Acknowledgment. This work is supported by the Research Program of Hebei Educational Committee Grant No. QN2015109 and Research of Yanshan University for Youths Grant No. 15LGA009. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti and T. Wang, Supporting anonymous location queries in mobile environments with privacygrid, *Proc. of Int'l World Wide Web Conf.*, 2008.

[2] Tyagi and A. Kumar, Location privacy preserving techniques for location based services over road networks, *International Conference on Communication and Signal Processing*, no.9, pp.1319-1326, 2015.

[3] H. Hu and J. Xu, Non-exposure location anonymity, *Proc. of IEEE Int'l Conf. Data Eng.*, 2009.

[4] B. Ying and D. Makrakis, Protecting location privacy with clustering anonymization in vehicular networks, *IEEE INFOCOM Workshop on Dynamic Social Networks*, 2014.

[5] M. Y. Jang, S.-J. Jang and J.-W. Chang, A new K-NN query processing algorithm enhancing privacy protection in location-based services, *IEEE the 1st Internation Conference on Moblie Services*, 2012.

[6] L. Yao, C. Lin, G. Liu, F. Deng and G. Wu, Location anonymity based on fake queries in continuous location-based services, *The 7th International Conference on Availability, Reliability and Security*, 2012.

[7] X. Pan, J. Xu and X. Meng, Protecting location privacy against location-dependent attacks in mobile services, *IEEE Trans. Knowledge and Data Engineering*, 2012.

[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K. Tan, Private queries in location based services: Anonymizers AreNot necessary, *Proc. of ACM SIGMOD Int'l Conf. Management of Data*, 2008.

[9] B. Bamba, L. Liu and E. Yigitoglu, Road network-aware anonymization in mobile systems with reciprocity support, *Computer Communication and Networks*, 2015.

[10] X. Pan and X. Meng, Preserving location privacy without exact location in mobile services, *Frontiers of Computer Science*, pp.317-340, 2013.
[11] Y. Che, Q. He, X. Hong and K. Chiew, X-region: A framework for location privacy preservation in mobile peer-to-peer networks, *International Journal of Communication Systems*, pp.167-186, 2013.
[12] B. Palanisamy and L. Liu, Mobimix: Protecting location privacy with mix-zones over road networks, *Proc. of 2011 IEEE 27th International Conference on Data Engineering*, pp.494-505, 2011.
[13] J. Meyerowitz and R. Choudhury, Hiding stars with fireworks: Location privacy through camouflage, *Proc. of MOBICOM*, pp.345-356, 2009.
[14] J. Bao, H. Chen and W. S. Ku, Pros: A peer-to-peer system for location privacy protection on road networks, *ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp.552-553, 2009.
[15] H. J. Cho, S. J. Kwon and R. Jin, A privacy-aware monitoring algorithm for moving k-nearest neighbor queries in road networks, *Distributed and Parallel Databases*, pp.319-352, 2015.
[16] T. Wang and L. Liu, Privacy-aware mobile services over road networks, *VLDB Endowment*, pp.1042-1053, 2009.
[17] Y.-K. Kim, A. Hossain, A.-A. Hossain and J.-W. Chang, Hilbert-order based spatial cloaking algorithm in road network, *Concurrency and Computation: Practice and Experience*, pp.143-158, 2013.
[18] C. Li and B. Palanisamy, ReverseCloak: Protecting multi-level location privacy over road networks, *Proc. of the 24th ACM International on Conference on Information and Knowledge Management*, pp.673-682, 2015.
[19] C. Ma and C. Zhou, A Voronoi-based location privacy-preserving method for continuous query in LBS, *International Journal of Distributed Sensor Networks*, p.17, 2015.
[20] Y. Wang and Y. Xia, A fast privacy-preserving framework for continuous location-based queries in road networks, *Journal of Network and Computer Applications*, pp.57-73, 2015.
[21] P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias, Preserving location-based identity inference in anonymous spatial queries, *IEEE Trans. Knowledge and Data Eng.*, vol.19, no.12, pp.1719-1733, 2007.
[22] E. G. Hoel and H. Samet, Efficient processing of spatial queries in line segment databases, *Proc. of Int'l Symp. Advances in Spatial Databases (SSD)*, 1991.
[23] H. Kido, Y. Yanagisawa and T. Satoh, An anonymous communication technique using dummies for location-based services, *Proc. of ICPS*, 2005.
[24] T. Brinkhoff, A framework for generating network-based moving objects, *GeoInformatica*, vol.6, no.2, pp.153-180, 2002.