Protection of Location Privacy in Continuous LBSs against Adversaries with Background Information

Ben Niu*, Sheng Gao†, Fenghua Li*¶, Hui Li‡ and Zongqing Lu§
*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, China
†School of Information, Central University of Finance and Economics, Beijing, China
‡National Key Laboratory of Integrated Networks Services, Xidian University, China
§Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, USA
*{niuben, lfh}@iie.ac.cn, †sgao555@gmail.com, ‡lihui@mail.xidian.edu.cn, §zongqing@cse.psu.edu
¶Corresponding author

***Abstract*—Privacy issues in continuous Location-Based Services (LBSs) have gained attractive attentions in literature over recent years. In this paper, we illustrate the limitations of existing work and define an entropy-based privacy metric to quantify the privacy degree based on a set of vital observations. To tackle the privacy issues, we propose an efficient privacy-preserving scheme, DUMMY-T, which aims to protect LBSs user's privacy against adversaries with background information. By our Dummy Locations Generating (DLG) algorithm, we first generate a set of realistic dummy locations for each snapshot with considering the minimum cloaking region and background information. Further, our proposed Dummy Paths Constructing (DPC) algorithm guarantees the location reachability by taking the maximum distance of the moving mobile users into consideration. Security analysis and empirical evaluation results further verify the effectiveness and efficiency of our DUMMY-T.**

I. Introduction

Location-Based Services (LBSs) have become increasingly popular over recent years. Users with mobile devices such as smartphones or tablets can download location-based applications from Apple Store or Google Play Store, and install them locally to learn the environments and enjoy the convenience provided by the LBS servers. Generally, there are two types of LBSs, namely, *snapshot* and *continuous* LBSs (cLBSs for short). For example, mobile users can look for the hotels or banks nearby (*snapshot* LBSs), and go there under navigation of the GPS-based applications (cLBSs).

However, mobile users always need to continuously submit their location-related queries to the untrusted LBS server, who can obtain all the information about users such as where they are at which time, and what they are doing, etc., and who may also track users in various ways or release their personal data to third parties. These privacy threats become more seriously in the continuous scenario. Thus, we need to pay more attention to user's privacy in cLBSs.

To address such privacy issues, many approaches [1], [2], [3], [4], [5], [6], [7], [8], [9] have been proposed from the research community over recent years. They can be roughly categorized into two main types in terms of system architecture, including 1) trusted anonymizer-based approaches [4], [5], [?] and 2) client-based approaches [1], [3], [2], [10]. Technically, besides some techniques such as Mix-zone [11], vehicular mix-zone [7], [8], [9] and path confusion [6], spatial cloaking [3], [4] and dummy routes [1], [2] are two popular techniques to provide location privacy protection for mobile users in LBSs. They can be achieved through group-based P2P [3], distortion-based [5], prediction-based [4] and randomly dummy choosing-based [2] approaches. However, we believe that most of existing approaches fail in one or more of the following arguments, 1) deeply relying on the trusted anonymizer which may lead to serious privacy concern such as single point of failure; 2) hardly balancing the tradeoff between system performance and the size of cloaking regions, for instance, bigger cloaking regions bring higher privacy level but more system overhead and vice versa; 3) failing to make a full consideration on the *background information* [12], [13] in adversaries' hands.

In this paper, we consider the aforementioned arguments and propose a Location Privacy Metric for cLBSs scenario to measure the privacy level. Further, with combining spatial cloaking and dummy-based techniques, we design an efficient privacy-preserving location protecting scheme for cLBSs users against adversaries with background information, called *DUMMY-T*. The contributions of this paper are as follows.

- We make a set of observations based on two existing approaches, which may lead to serious privacy attacks performed by adversaries with *background information*.
- We define an entropy-based Location Privacy Metric, which measures the privacy level of *k-anonymity*-based solutions considering the privacy concerns from our observations.
- We propose a privacy-preserving scheme, termed *DUMMY-T*, which provide *k-anonymity* for cLBSs users. By DLG algorithms, we first generate a set of realistic dummy locations for each snapshot that guarantees the minimum cloaking region and resists from attacks performed by adversaries with *background information*. Further, with DPC algorithm, we connect the dummy locations together into the dummy paths with considering the location reachability.
- Analytical and simulation results show that our scheme can achieve our objectives effectively and efficiently.

The rest of this paper is organized as follows. Section II reviews the related work. Section III gives the preliminaries. Following in Section IV, we describe the details of our

978-1-4673-8579-4/16/$31.00 ©2016 IEEE

proposed system. Then, the security analysis is provided in Section V. Finally, we evaluate the performance and draw the conclusion in Section VI and VII, respectively.

II. Related Work

A. Metrics for Location Privacy

k-anonymity [14] is a well used metric to measure user's location privacy in LBSs, based on which linking two pseudonyms of a particular user and distinguishing the paths along which a user may travel has been investigated in [15] and [6], respectively. Later, as an extension of *k-anonymity*, entropy-based metrics [15], [6], [13], [16] and distortion-based metrics [17] have been widely adopted. To quantify the location privacy, we should find out how accurately an adversary might infer about the location information. A well-known metric for privacy is *k-anonymity* [2], [4], which aims to improve the uncertainty of location privacy by hiding the real location into other $k-1$ with dummies [2] or history data [4]. However, they failed to consider *background information* such as query probability or road density. Thus, we need to design a new metric for user's location privacy with full consideration of *background information*.

B. Protecting Location Privacy

A significant amount of researches has been proposed on protecting location privacy for mobile users in LBSs, including spatial cloaking, dummy routes, mix-zone and path confusion etc., which are achieved through either trusted anonymizer [4], [5] or mobile client [1], [3], [2]. With the trusted anonymizer, mobile users in [5] report their locations to the anonymizer, which takes users' movement directions and velocities to construct minimized cloaked spatial regions to achieve *k-anonymity*. However, the single point of failure happens once the anonymizer is compromised. Xu *et al.* [4] explored each individual's historical footprints to achieve *k-anonymity*, instead of real time locations. Unfortunately, user's privacy degree is still related to the employed anonymizer. Later, Mix-zone [7], [8] is proposed to achieve the desired anonymity degree by periodically changing the pseudonym. However, the employed *mix-router* acts as another kind of trusted anonymizer, and may pose user's privacy in danger. Without the trusted anonymizer, Kido *et al.* [1] proposed to use dummy routes to achieve anonymity. However, they only focused on reducing system overhead but ignored the *background information*, and thus, the desired anonymity degree cannot be guaranteed. Similarly, You *et al.* tried to generate a set of realistic dummies in terms of three metrics, however, the *background information* was also ignored. For the technique details of these approaches, we refer the readers to a recent survey [18].

III. Preliminaries

A. Basic Concepts

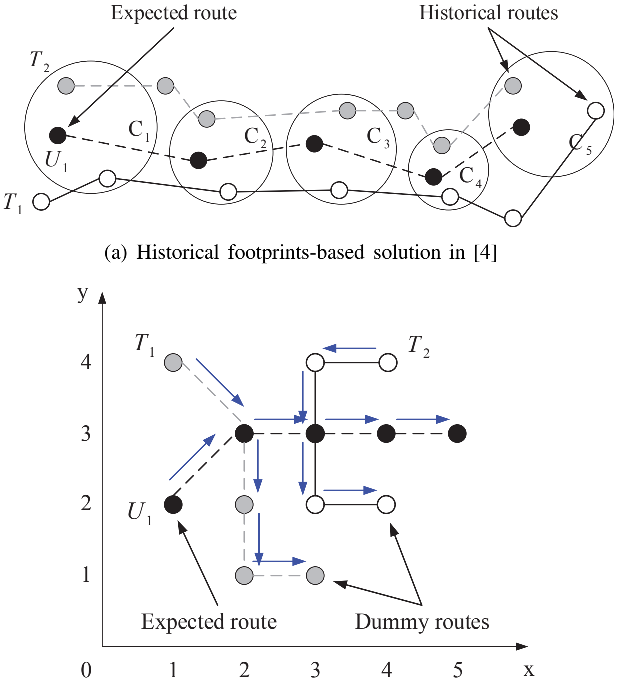
Background Information: In our work, this kind of information is limited to users' query probability information in the local map. Specifically, we divide a local map into a set of cells (e.g., $n \times n$ cells), a user's query probability is represented as the probability that the user submits location-based queries on a particular cell.

Minimum Cloaking Region (MCR): Suppose we decompose all the locations within a cLBSs (termed as route) into several snapshots (i.e., n). With spatial cloking technique, the user in each snapshot should construct a cloaking region, which covers other $k-1$ users to confuse the LBS server. This term thus aims to limit the minimum size of the cloaking region in all the snapshots due to the privacy concern.

Location Reachability (LR): For any current location l_{t_i} in either real route or dummy paths, the next location $l_{t_{i+1}}$ should be reachable based on the user's velocity.

B. Motivation

Our work is motivated by a set of observations on two existing location privacy protecting schemes, which can be found in Fig. 1(a) and 1(b), respectively. We first review a historical footprints-based solution [4] shown in Fig. 1(a), which uses the historical footprints to predict the user's movement and protect the location privacy in cLBSs. In this figure, U_1 represents the expected route, which can be further divided into several snapshots (i.e., 5 snapshots in the whole route) with different timestamps. T_1 and T_2 are two historical routes. In each snapshot, C_i is the cloaking region which covers the user's current location and other two locations of the historical routes for anonymous purpose. Based on these knowledge, we illustrate our observations. **Observation I:** This scheme is deeply relied on a fully trusted location anonymizer, which may cause serious problems such as single point of failure from either system performance or user's privacy points of view. **Observation II:** Due to the system overhead issue, the authors try to minimize the size of the cloaking region as much as possible. However, user's location privacy may be revealed by a too small cloaking region (i.e., C_4, which means that these three locations may be targeted into a very small area such as a bar at a downtown area). Further, with more historical routes collected, there may be more number of cloaking regions like C_4, the user's location privacy is thus revealed. **Observation III:** It is hard to balance the system performance with privacy level, since less historical routes may lead to bigger cloaking regions, while more historical routes may cause the privacy problem mentioned in **Observation II**. Similar to Fig. 1(a), we review another dummy-based solution [2] shown in Fig. 1(b), which avoids the heavy storage overhead and the single point of failure problem caused by the central server. To achieve *k-anonymity* in cLBSs, the real user construct another k-1 dummies by connecting a set of dummy locations. However, due to the ignorance on the *background information*, the desired privacy level may not be achieved effectively. **Observation IV:** Since the chosen dummy locations in the snapshots may fall at some unlikely locations such as lakes, swamps, and rugged mountains, the two dummies T_1 and T_2 may be easily filtered out by the adversaries with the *background information*. **Observation V:** This scheme prefers more intersections between routes from the system performance point of view. However, we argue that,



(a) Historical footprints-based solution in [4]

(b) Dummy-based solution in [2]

Fig. 1. Our motivations on the limitations of existing approaches

more intersections may cause the privacy problem mentioned in **Observation II**. As a result, the user's moving trend may be disclosed.

This work is motivated by all these five observations on the two kinds of location privacy-preserving solutions.

C. Our Basic Idea

To tackle the aforementioned problems, the main purpose of our scheme is to design an efficient scheme, which fully considers the *background information* in the whole process and achieves several privacy properties in terms of minimum cloaking region guarantee and reachability within each dummy path. We illustrate our idea by a simple example shown in Fig. 2. Specifically, a particular user *Alice* tries to protect her privacy under *3-anonymity*, the whole process can be divided into 5 snapshots based on the increasing timestamps t_1, t_2, t_3, t_4 and t_5. The corresponding cloaking region in each snapshot is denoted as C_1, C_2, C_3, C_4 and C_5. The route in blue is the user's real route, and the routes in gray and yellow represent our carefully generated dummy paths. For each snapshot, DLG algorithm generates a set of dummy locations which cannot be distinguished from others easily, while guaranteeing that all the selected dummy locations within each snapshot should not fall into a too small region (i.e., a bar area). Further, DPC algorithm connects the corresponding dummy locations into several dummy paths with considering the reachability, which guarantees that the next location can be reached from current location in each path according to user's velocity.

IV. Our Proposed DUMMY-T

In this section, we first present the system architecture of our proposed *DUMMY-T*, then we define our location privacy metric, show the dummy location generating algorithm and dummy paths constructing algorithm, respectively.

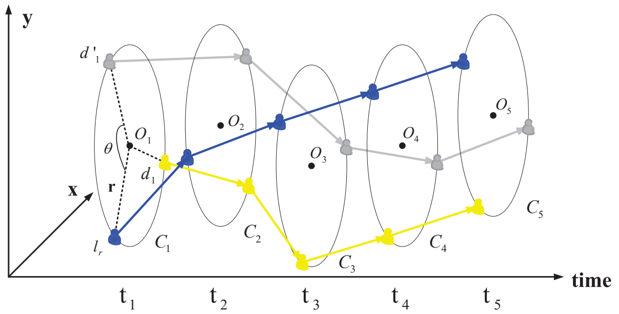


Fig. 2. Our basic idea

A. System Architecture

Our proposed scheme, termed *DUMMY-T*, uses a distributed architecture. Mobile users in our scheme work independently and connect to the LBS server through cellular networks, such as 3G/4G. When a particular user *Alice* needs LBSs, she runs our scheme locally to generate several dummy paths around the real route, then submits them together to the LBS server to obtain service data. Generally, we separate our scheme into two main algorithms, Dummy Locations Generating (DLG) algorithm and Dummy Paths Constructing algorithm (DPC).

B. Location Privacy Metric

Basically, our Location Privacy Metric (LPM) is defined based on the location entropy, which can be seen as the uncertainty in determining the current location of an individual [19] from all the candidates. It can be computed as

$$H = -\sum_{j=1}^{k} p_j \cdot \log_2 p_j, \tag{1}$$

where p_j means the probability assigned on each possible location and the sum of all probabilities p_j is 1.

To further adopt it into the cLBSs scenarios, we recall the example shown in Fig. 2 and extend it by the following steps.

(i) We compute the entropy for each snapshot by

$$H_{C_i} = -\sum_{j=1}^{k} p_j^i \cdot \log_2 p_j^i, \tag{2}$$

where p_j^i represents the normalized query probability of the anonymous set (i.e., p_{l_r}, p_{d_1} and $p_{d'_1}$ in the first snapshot in our example). This term describes the uncertainty to distinguish the user's real location from all the possible locations in a single snapshot.

(ii) We know that the maximum entropy is achieved when all the k possible locations have the same probability $\frac{1}{k}$, where the maximum entropy will be $H_{C_i}^{max} = \log_2 k$. Ideally, we aim to achieve the maximum entropy in each snapshot, therefore, we compute the average entropy as

$$\overline{H_C} = \frac{\sum_{i=1}^{n} H_{C_i}}{n}, \tag{3}$$

where n is the total number of snapshots.

(iii) Finally, we obtain the variance of the average entropy in all the snapshots by

$$\begin{aligned}\sigma^2 &= E[(H_C - \overline{H_C})^2] \\ &= \frac{\sum_{i=1}^{n}(H_C - \overline{H_C})^2}{n}.\end{aligned} \tag{4}$$

Obviously, due to the differences of uncertainty between different snapshots, the lower the σ^2 is, the higher privacy level will be.

C. Dummy Locations Generating Algorithm

Let's recall the example in Fig. 2, the user's route can be determined easily (i.e., the shortest route provided by submitting the destination to GPS device), which is shown in blue. We now use a simple example shown in Fig. 3 to show how DLG algorithm works under a particular snapshot (C_1 at the timestamp t_1). Suppose the user-defined Minimum Cloaking Region (MCR) is denoted as A_{min}, we then compute the corresponding minimum radius as

$$r_{min} = \sqrt{\frac{A_{min}}{\pi}}. \tag{5}$$

For a particular snapshot C_i, based on the real user's location l_r^i, we define a virtual circle with a randomly chosen center O_i and of radius R_i, which can be found in Fig. 3(a) and satisfies

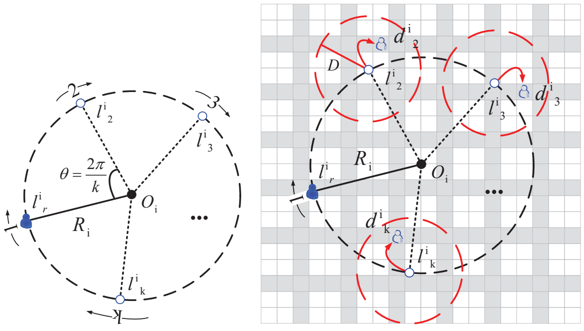
$$\begin{aligned}R_i &= |O_i\ l_r^i| \\ &= r_{min} \cdot \delta_i,\end{aligned} \tag{6}$$

where δ_i is a user defined parameter and satisfies $|\delta_i - 1| = \varepsilon_i$. Note that, ε_i is a small positive number such as 0.05 or 0.1. Next, we partition this virtual circle into k parts with equal angle $\theta = \frac{2\pi}{k}$ (equal angle is defined here to guarantee that any two routes in a particular snapshot cannot be too close to each other), and find out the corresponding points $l_2^i, l_3^i, \cdots, l_k^i$ with the clockwise direction, respectively. Further, in Fig. 3(b), we blur the obtained points $l_2^i, l_3^i, \cdots, l_j^i, \cdots l_k^i$ into their final positions $d_2^i, d_3^i, \cdots, d_j^i, \cdots, d_k^i$ with considering the *background information*. Specifically, for each obtained point (i.e., l_j^i), we first define an offset D (i.e., 0.1 or 0.2 mile), search and find out the proper cells, which have similar query probability with the real user's, within the circular region with the center point l_j^i and of radius D. Then, we can obtain a set of candidates (i.e., the cells in gray within the red dashed circle in our example, denoted as L_j^i), which can guarantee the privacy level in terms of LPM (shown in Eq. 4). To improve the system performance, we can either limit the size of the candidate set or reduce the offset D.

D. Dummy Paths Constructing Algorithm

With the candidate sets of all the snapshots in hand, we consider the Location Reachability (LR) property and design DPC algorithm to find out the optimal dummy paths to achieve the *k-anonymity*.

Generally, the first snapshot can be determined easily through DLG algorithm and other snapshots are determined by DPC algorithm as in Algorithm 1. To consider LR property, we define a parameter $Dis_{t_i}^{max}$, which aims to give a limitation on the maximum distance that a user can move from the current location (in current snapshot) to the next. It can be computed as



(a) Step 1

(b) Step 2

Fig. 3. Dummy locations generating algorithm

$$Dis_{t_i}^{max} = v_{t_i} \times (t_i - t_{i-1}), \tag{7}$$

where v_{t_i} indicates the user's corresponding velocity at a particular snapshot when the timestamp is t_i. We also define the dummy path $\mathcal{D}_j$ to achieve *k-anonymity*. DPC algorithm is to fill up $\mathcal{D}_j$ with carefully selected dummy locations. For each obtained candidate set L_j^i from DLG algorithm, we filter out some unreachable locations in terms of $Dis_{t_i}^{max}$, then randomly choose one location from the remaining set and add it into the final dummy path $\mathcal{D}_j$. Through this way, we can obtain $k-1$ sets of dummy paths $\mathcal{D}_2, \cdots, \mathcal{D}_k$, respectively.

Algorithm 1: Dummy Paths Constructing Algorithm

```
Input  : the candidate sets $L_j^i$, $n$, $k$, $t_i$, user's velocity $v_{t_i}$
Output: $k-1$ dummy paths $\mathcal{D}_2, \cdots, \mathcal{D}_k$
initiates $\mathcal{D}_j = \emptyset$;
for $(i = 2; i < n; i++)$ do
    computes $Dis_{t_i}^{max} = v_{t_i} \times (t_i - t_{i-1})$;
    for $(j = 2; i < k; j++)$ do
        adds $d_j^{i-1}$ into dummy path $\mathcal{D}_j$;
        for $(\forall\ l_m \in L_j^i)$ do
            computes $d_m = dis(d_j^{i-1}, l_m)$;
            if $(d_m > Dis_{t_i}^{max})$ then
                removes $l_m$ from $L_j^i$;
            end
        end
        randomly chooses a location from $L_j^i$ and adds it into
        dummy path $\mathcal{D}_j$;
    end
end
outputs $\mathcal{D}_2, \cdots, \mathcal{D}_k$.
```

V. Security Analysis

We consider two types of adversaries in our work, *passive adversary* and *active adversary*. Attacks from *passive adversary* are always based on eavesdropping messages from the communication channels, then modify, replay or inject these messages. Actually, these kinds of attacks can be avoided easily by employing some cryptography tools such as Public Key Infrastructure (PKI). We thus focus on avoiding attacks from the *active adversary*, who can compromise LBS servers and obtain all the information of mobile clients, such as *colluding attacks* and *inference attacks*, which may cause serious privacy problems.

A. Resistance to Colluding Attacks

Adversaries may collude with some users to learn extra information than allowed.

Theorem 1. *Our scheme is colluding attack resistant.*

Proof: Colluding attack always happen between a set of users. However in our scheme, since there is no interaction with any other users, colluding with users has no effect on other users, thus, our scheme is colluding attack resistant. ■

The best case to this kind of adversaries is that he can get all the information by compromising LBS server, then he becomes an *active adversary* to perform *inference attack*.

B. Resistance to Inference Attack

Since we consider the untrusted LBS server as the *active adversary* to perform *inference attack*, he can obtain knowledge by monitoring all the users in the system, including their interests, current query as well as the query history, etc. His aim then is to target an observed route to the real user.

Theorem 2. *Our scheme is inference attack resistant.*

Proof: To perform the *inference attack*, the *active adversary* may use any possible ways, such as 1) analyzing the minimum cloaking region (see in our **Observation II, V** in Sec III-B) or 2) filtering locations with *background information* (see in **Observation IV**) in each snapshot. However, for each snapshot in our scheme, due to the minimum cloaking region A_{min} is considered at the beginning of our DLG algorithm, the size of each constructed cloaking region is guaranteed to be similar to A_{min}. As a result, the adversaries cannot increase the success ratio on determining the dummy locations or dummy paths by analyzing each cloaking region. On the other hand, we use a location blurring phase in our DLG algorithm to fully consider the *background information*. By blurring each dummy location l_j^i into the final position d_j^i, which has similar query probability with the real user's, the adversaries can hardly distinguish user's real location from other $k-1$ dummies, even with the *background information*. Therefore, *k-anonymity* can be further guaranteed. ■

VI. Performance Evaluations

A. Simulation Setup

To obtain the route data, we first analyze the Borlange Data Set, which was collected over two years as part of an experiment on traffic congestion that took place in Borlange (see [20] for more details), and randomly choose 5000 routes from the central part (about $8km \times 8km$) of this map. We then divide this area into a grid with 160×160 cells and compute the *background information* based on the frequency information appeared in each cell.

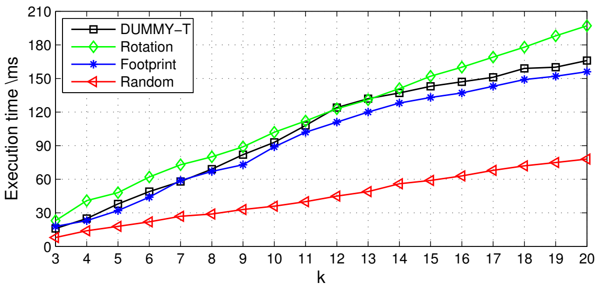


Fig. 4. k vs. execution time

There are several parameters used in our evaluation. k is related to *k-anonymity*, and is commonly set from 3 to 20. We compare our proposed *DUMMY-T* with four other schemes. The *Random* scheme represents the dummy selection algorithm in [1], which randomly chooses dummies. The *Optimal* scheme shows the optimal results of *k-anonymity* in theory. The *Rotation* scheme indicates the rotation-based dummy selection algorithm mentioned in [2]. The *Footprint* scheme [4] is a prediction-based scheme which achieves *k-anonymity* for mobile users based on the historical route data.

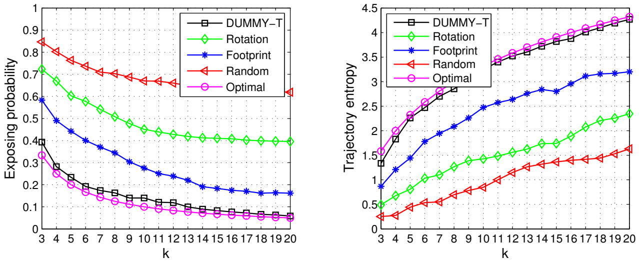
B. Evaluation Results

1) k vs. execution time: We first show the relationship between execution time and k when using different schemes. In Fig. 4, the *Random* scheme [1] performs better than other schemes since it does not focus on improving the user privacy. For the other results in this figure, our *DUMMY-T* provides competitive performance compared to the *Rotation* scheme [2] and the *Footprint* scheme [4]. Note that, in this experiment, the offset D is set to 300 meters, which brings more searching overhead when determining the final position of each chosen dummy location in Fig. 3(b). That is to say, the execution time can be further reduced once we decrease the offset D.

2) k vs. user privacy: Then we evaluate the effect of varying k on the exposing probability of the user's real route, which can be computed as

$$\overline{\mathbb{PR}_{real}} = \frac{\sum_{i=1}^{n} p_{real}^{i}}{n}, \tag{8}$$

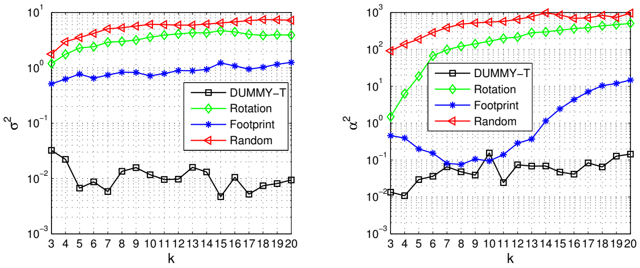
where p_{real}^{i} represents the query probability of the cell that real user located in each snapshot. From Fig. 5(a), we can see our *DUMMY-T* is very close to the optimal value in each tested k and outperforms other existing schemes. Obviously, the performance of *Random* scheme is the worst due to the ignorance on the *background information*. Comparing the *Rotation* [2] scheme with *Footprint* [4] scheme, the latter one is better, the reason is that *Footprint* collects user's historical data to achieve anonymity and locations on each historical routes are solid, which guarantees the anonymity degree in some sense. Although route rotation phase is employed in their scheme to guarantee the similarity of newly generated dummy routes, the *background information* is still ignored. Therefore, the exposing probability of the real route increases. We also



(a) k vs. exposing probability

(b) k vs. entropy

Fig. 5. k vs. user privacy



(a) k vs. σ^2

(b) k vs. α^2, $A_{min} = 1km^2$

Fig. 6. k vs. σ^2 and k vs. α^2

show the average entropy of each route in terms of Eq. 3. Same as the exposing probability, Fig. 5(b) shows the performance of different schemes and *DUMMY-T* still outperforms *Random*, *Rotation* and *Footprint*.

3) k vs. σ^2: Next, we use Eq. 4 to evaluate the performance of the variance of the average entropy, which is closely related to the user's privacy. The optimal result is that the entropy of each snapshot is $\log_2 k$, and $\sigma^2 = 0$. As a result, the adversary can only distinguish the user's real route randomly. As shown in Fig. 6(a), we can clear see the better performance provided by our *DUMMY-T*.

4) k vs. α^2: Finally, we evaluate the impact of different k on the variance to user defined A_{min}, it can be computed as

$$\alpha^2 = \frac{\sum_{i=1}^{n}(A_{C_i} - A_{min})^2}{n}, \tag{9}$$

where A_{C_i} denotes the size of the i^{th} snapshot C_i. Generally, higher α^2 means the size of the cloaking region in some snapshots may be too big than user defined A_{min}, and some of them may be too small. Therefore, they may cause serious privacy problems as illustrated in our **Observation II** in Sec. III-B. Fig. 6(b) shows the evaluation results of different schemes. Specifically, our *DUMMY-T* works well, and *Footprint* is better than other schemes due to the utilization on the historical data, which guarantees that the cloaking region cannot be too big.

VII. Conclusions

In this paper, we presented a novel privacy-preserving scheme to protect user privacy for mobile users in cLBSs. With several observations, we pointed out the serious privacy problems in existing solutions. Based on our newly defined location privacy metric, we proposed an efficient privacy-preserving scheme, *DUMMY-T*. With considering the minimum cloaking region and *background information* may be disclosed, *DUMMY-T* first generates a set of realistic dummy locations in each snapshot, and then, connected them into dummy paths by taking the location reachability property into consideration.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (61502489) and the National High Technology Research and Development Program of China (863 Program) (2015AA016007, 2012AA013102).

References

[1] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *IEEE ICPS 2005*.

[2] T.-H. You, W.-C. Peng, and W.-C. Lee, "Protecting moving trajectories with dummies," in *IEEE MDM 2007*.

[3] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in *ACM SSTD 2007*.

[4] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services," in *IEEE INFOCOM 2008*.

[5] X. Pan, X. Meng, and J. Xu, "Distortion-based anonymity for continuous queries in location-based mobile services," in *ACM GIS 2009*.

[6] J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: Location privacy through camouflage," in *ACM MobiCom 2009*.

[7] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones," in *ACM PETS 2009*.

[8] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in *IEEE ICDE 2011*.

[9] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks." *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[10] R.-H. Hwang, Y.-L. Hsueh, and H.-W. Chung, "A novel time-obfuscated algorithm for trajectory privacy protection," *Services Computing, IEEE Transactions on*, vol. 7, no. 2, pp. 126–139, April 2014.

[11] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "Trpf: A trajectory privacy-preserving framework for participatory sensing," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 6, pp. 874–887, June 2013.

[12] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *IEEE INFOCOM 2013*.

[13] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *IEEE INFOCOM 2014*.

[14] L. Sweeney, "k-anonymity: a model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[15] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in *ACM MobiSys 2007*.

[16] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *IEEE INFOCOM 2015*.

[17] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *IEEE Security and Privacy 2011*.

[18] C.-Y. Chow and M. F. Mokbel, "Trajectory privacy in location-based services and data publication," *SIGKDD Explor. Newsl.*, vol. 13, no. 1, pp. 19–29, Aug. 2011.

[19] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *ACM PETS 2003*.

[20] E. Frejinger, "Route choice analysis: data, models, algorithms and applications," Ph.D. dissertation, Lausanne, 2008.