A Novel Dummy-based Mechanism to Protect Privacy on Trajectories

Xichen Wu
School of Computer Science and Technology
University of Science and Technology of China
Hefei, Anhui, China
Email: wxc422@mail.ustc.edu.cn

Guangzhong Sun
School of Computer Science and Technology
University of Science and Technology of China
Hefei, Anhui, China
Email: gzsun@ustc.edu.cn

***Abstract*—In recent years, wireless communication technologies and accurate positioning devices enable us to enjoy various types of location-based services. However, revealing users location information to potentially untrusted LBS providers is one of the most significant privacy threats in location-based services. The dummy-based privacy-preserving approach is a popular technology that can protect real trajectories from exposing to attackers. Moreover, it does not need a trusted third part, while guaranteeing the quality of service. When user requests a service, dummy trajectories anonymize the real trajectory to satisfy privacy-preserving requirements.**

In this paper, we propose a new privacy model that includes three reasonable privacy metrics. We also design a new algorithm named adaptive dummy trajectories generation algorithm (ADTGA) to derive uniformly distributed dummy trajectories. Dummy trajectories generated by our algorithm can achieve stricter privacy-preserving requirements based on our privacy model. The experimental results show that our proposed algorithm can use fewer dummy trajectories to satisfy the same privacy-preserving requirement than existing algorithms, and the distribution of dummy trajectories is more uniformly.

***Keywords*-Trajectory privacy; Location-based services; Dummy-based anonymization**

I. Introduction

Advances in wireless communication technologies and smart mobile devices equipped with GPS (Global Positioning System) receivers have led to a ubiquitous utility of Location Based Services (LBSs) in our daily life. In LBSs, users send queries with their precise location information to LBS providers, and then they can acquire the corresponding query results. For example, someone intends to find the nearest restaurant or hospital. After sending a query, he/she will acquire the results. However, privacy leakage caused by these services should be attached most importance to. In these services, if service providers or attackers can steal the query message, the entire query involving some sensitive information may be disclosed to them.

To address the problem, Kido et al. [1] proposed a dummy-based location privacy mechanism to avoid privacy leakage. In the proposed technique, fake locations called dummies are generated, and then these dummies are sent to the LBS provider together with the real user location. So the LBS provider has difficulty to distinguish the real location from dummies. The mechanism can be embedded in user mobile devices, which does not need a trusty intermediate server for collection and anonymization. Moreover, this approach can assure the quality of LBS, as the results are based on precise location.

In this paper, we propose a novel privacy-preserving model which utilizes more reasonable and accurate privacy metrics to fulfill the requirement preserving the user location and trajectory privacy. In addition, we develop a novel algorithm, namely Adaptive Dummy Trajectories Generation Algorithm (ADTGA). It generates dummy trajectories based on user privacy model so that the distribution of dummies can be more uniform. The experiment results show that our proposed algorithm can generate fewer dummy trajectories to fulfill the same privacy requirement than priori approach [2], [3], and the trajectories is more-distributed on the map.

The rest of this paper is organized as follows. Section II describes related work about dummy-based location privacy and other valuable methods. Section III presents details of our proposed privacy model and Section IV describes the process of our Adaptive Dummy Trajectories Generating Algorithm. Section V shows our experiment study and at last Section VI concludes the paper with a summary.

II. Related Works

A wealth of studies has been carried out on location and trajectory privacy. Generally speaking, there are three common approaches that are spatial cloaking, mix-zones and dummy trajectories.

Firstly, spatial cloaking techniques [4]–[6] need a fully-trusted third part called location anonymizer which is located between mobile devices and LBS providers. In order to satisfy the user-specified k-anonymity requirement and minimum spatial region area, the location anonymizer is used to collect users locations and transform their locations into more spacious cloaked spatial region.

Secondly, in the mix-zones approach [7]–[9], when user enter a mix-zone, their fake identification is converted into a new and unused pseudonym. Moreover, when user is in the mix-zone he/she need not send any location information to the LBS provider. Hence an attacker cannot distinguish user u from any other users who were located in the same

978-1-4799-4274-9/14 $31.00 © 2014 IEEE
DOI 10.1109/ICDMW.2014.122

mix-zone at the same time. As usually, the mix-zone should also meet the demand of k-anonymity.

The last approach is the dummy-based location privacy technology. Without trusted third parts or LBS providers, Kido et al. [1] proposed a new anonymous communication technique letting users send their real location with dummies to the LBS provider in order to protect the location privacy.

In papers [10]–[12], authors focused on the need on the real environment considering physical constraints, and proposed the novel dummy generation algorithms called Dum-Grid and Dum-P [10], [11]. Dum-Grid generates dummies around the user in a grid pattern, while Dum-P assures a more realistic mobility model to generate dummies along with the user movements. Then an improved version named Dum-P-Cycle was proposed in paper [12] to solve the insufficient of requirement for location privacy. Privacy Area Aware (PAD) [13] takes the amount of the real location and the dummies into account, which is more appropriate in spatial contexts than purely k-anonymity based methods.

Our work is based on the papers [2], [3]. In the paper [2], authors were guided by privacy profile and proposed two schemes generating dummies in consistent movement patterns. Besides, Lei et al. [3] were inspired by the two schemes and then proposed a hybrid scheme called *k*-intersection scheme.

III. Privacy Model

This section defines the notion and assumption in trajectory privacy-preserving problem, then the detail of privacy model is presented finally.

A. Assumption and Definition

We assume there is no trusted third part and the LBS provider is not fully-trusted. Thus, location anonymization is processed on user's mobile devices. In order to simplify our discussion, we also assume that users move between the uniform grids. A grid is identified as (x, y), where x presents horizontal ordinate of the grid, and y presents vertical ordinate.

At time slot t, the user u_i wants to request a service, so he/she will send a message M to the LBS provider. The message M can be expressed in following formulation (1).

$$M = \{u_i, \langle L_i^t, L_{d1}^t, L_{d2}^t, ..., L_{dn}^t\rangle\} \tag{1}$$

Where u_i is the users pseudonym; L_i^t is his/her real location at time slot t, which is a grids identification (x_i, y_i); $L_{d1}^t, L_{d2}^t, ..., L_{dn}^t$ are fake locations at time slot t of n dummies, and the identification of every location is the same as the user's real one.

After user u_i sends m messages, his/her trajectory is formulated as $T_i = \{L_i^1, L_i^2, ..., L_i^m\}$. Accordingly, the dummy trajectory of d_x is formulated as $T_{dx} = \{L_{dx}^1, L_{dx}^2, ..., L_{dx}^m\}$.

B. Privacy Model

Our proposal privacy model consists of three privacy metrics: Δt-short term disclosure, long term disclosure and trajectories distance deviation . These metrics can be specified by user as privacy-preserving requirements. Intuitively, a stricter privacy-preserving requirement can lead to a lower probability of both real location and trajectory leakage.

*1) **Δt-Short term Disclosure (Δt-SD)**:* The Δt-short term disclosure denotes the degree of privacy-preserving for user real locations, namely the probability of locations exposed to attackers during a period time Δt. Priori work only considered the probability of exposed location at each time slot, but some unreasonable and inconsiderable situation may exist.

For example, we assume the real trajectory is $T_r = \{L^1, L^2, ..., L^m\}$, and the *i*-th location of dummy trajectory T_{d1} is the *(i-1)*-th location of the real trajectory, so it can be formulated as $T_{d1} = \{L^0, L^1, ..., L^{(m-1)}\}$. Another dummy trajectory T_{d2} is irrelevant to both T_r and T_{d1}, which is supposed as $T_{d2} = \{L'^1, L'^2, ..., L'^m\}$. If we consider the disclosure probability of location at each time slot instead of a period time Δt, the trajectory set $\{T_r, T_{d1}\}$ has the same probability as trajectory set $\{T_r, T_{d2}\}$ which are both $\frac{1}{2}$. Apparently, it is unreasonable because the disclosed locations of the former one should be much more than that of the latter.

Therefore, we propose the Δt-SD which considers the number of locations in a period time instead of at a time slot. And we can calculate the Δt-SD as the formulation (2).

$$\Delta t\text{-}SD = \frac{1}{m} \times \left[\sum_{i=0}^{\lfloor \frac{m}{\Delta t} \rfloor - 1} \frac{\Delta t}{D_{1+\Delta t \times i, (1+i) \times \Delta t}} + \frac{1}{\frac{D_{end+1,m}}{m-end}} \right] \tag{2}$$

Where *end*=$\lfloor \frac{m}{\Delta t} \rfloor \times \Delta t$, m is the number of location namely total time slot, $D_{i,j}$ presents the number of locations from *i*-th time slot to *j*-th time slot, specially $D_{i,i}$ presents the number of locations in the *i*-th time slot.

*2) **Long term Disclosure (LD)**:* This parameter denotes the degree of privacy-preserving for the real user trajectory, whose value is the probability of successfully identifying the trajectory. Given *n* trajectories, where *k* trajectories intersect with at less one other trajectory and the number of possible trajectories among these *k* trajectories is marked as T_k. The rest of $(n - k)$ trajectories do not have any intersection, so their number of possible trajectories is also $(n - k)$. Therefore the formulation of long term disclosure is the formulation (3).

$$LD = \frac{1}{T_k + (n - k)} \tag{3}$$

*3) **Trajectories Distance Deviation (TDD)**:* Previous model [2], [3] only consider the distance deviation between dummy trajectories generated and the real trajectory. So it would not distribute dummy trajectories uniformly on the map, and it is hard to protect the real trajectory.

To address the problem above, we propose the trajectories distance deviation (TDD) that presents the distance deviation among all the trajectories involving the real trajectory and dummy trajectories generated. Mark the real trajectory as T_{d0}, and the dummy trajectories as T_{dx} ($x \in [1,n]$). We assume there are $(n+1)$ trajectories, and each of them has *m* locations. Now we define the formulation of TDD as formulation (4).

$$TDD = \frac{1}{m} \times \frac{2}{n(n-1)} \times \sum_{i=0}^{n} \sum_{k=i+1}^{n} \sum_{j=1}^{m} dist(L_{di}^{j}, L_{dk}^{j}) \quad (4)$$

Where *m* is the number of locations in each trajectory, *n* is the number of dummy trajectories, and L_{di}^{j} denotes the location at time slot *j* of the trajectory T_{di}.

IV. Adaptive Dummy Trajectory Generation Algorithm

Given a privacy model involving the privacy metrics that are also the privacy-preserving requirements, and we can generate dummy trajectories to satisfy the privacy-preserving requirements. Sending these dummy trajectories to the LBS provider with the real trajectory can protect the real user trajectory from being exposed.

Previous algorithms generating dummy trajectories were proposed in literature [2], [3], which were named as random scheme, rotation scheme and *k*-intersected. These approaches can preserve the real trajectory from being exposed to attackers in the long run. However, they do not consider the influence by historical dummies. Besides, the movement pattern of dummy trajectories is the same as that of the real trajectory. Even if *k*-intersected scheme also has the threat that real trajectory is exposed to attackers, especially when sub-trajectories which should generated by rotation scheme are too long.

Therefore, we propose a new algorithm named Adaptive Dummy Trajectories Generation Algorithm (ADTGA) to solve these problems. Our proposal algorithm considers the influence of historical dummy trajectories when generating a new trajectory. It also includes a perturbation procedure to make the dummy trajectories distributed more uniformly on the map and to disturb attackers to observe the real trajectory pattern.

A. Design Policy

To focus on the influence of historical dummy trajectories when generating new dummy trajectory. Guided by trajectories distance deviation (TDD) defined in privacy model, we consider the distance deviation between the new dummy trajectory and all other trajectories. What's more, when calculating the distance deviation of n dummy trajectories that have been generated, we also consider the distance deviation among all the n dummy trajectories. The above points make it possible to fulfill our privacy metric TDD in privacy model.

Algorithm 1 : Generate adaptive dummy trajectories

Input: the real user trajectory *T*; perturbation degree *k* which is a percentage; and privacy metrics in privacy model: Δt-SD (marked as *TSD*), *LD* and *TDD*;

Output: *Dummies* which is the dummy trajectories generated set;

```
1:  $Dummies = \emptyset$;
2:  repeat
3:     $Candidate = \emptyset$;
4:     for each $\theta \in \{10°, 20°, ..., 350°\}$ do
5:        for $t \in [1, T]$ do
6:           $dummy = GenerateDummy(\theta, t)$;
7:           if dummy do not satisfy privacy metric TDD then
8:              continue;
9:           end if
10:          $adaptivedummy = Perturbation(dummy, k)$;
11:          append dummy to Candidate;
12:       end for
13:    end for
14:    for dummy in Candidate do
15:       Compute the $\Delta t$-SD and LD of dummy;
16:    end for
17:    Append dummy having the minimal metrics to Dummies;
18:    Compute $\Delta t$-SD and LD of all trajectories as tsd and ld;
19: until $tsd \geq TSD$ and $ld \geq LD$
20: return Dummies
```

Next, we discuss the perturbation procedure in our algorithm which reflects adaptability of the algorithm. Firstly, we select *k* locations from the new dummy trajectory just generated where *k* is a parameter specified by user; then move each location of *k* in the direction where there are fewer locations and trajectories. Note that the perturbed dummy trajectory should also fulfill the privacy requirements. As a result, dummy trajectories can be placed in the region where there are fewer trajectories.

B. Algorithm Procedure

Algorithm 1 shows the procedure of our algorithm ADTGA. The inputs of algorithm are the real user trajectory *T*, perturbation degree *k* and the three metrics in privacy model as privacy-preserving requirements. At the end of the algorithm, dummy trajectories generated are outputted.

The algorithm first sets the *Dummies* and *Candidate* as empty set (line 1, 3). Next, it enumerates rotation angels and rotation locations to create the candidate in which the

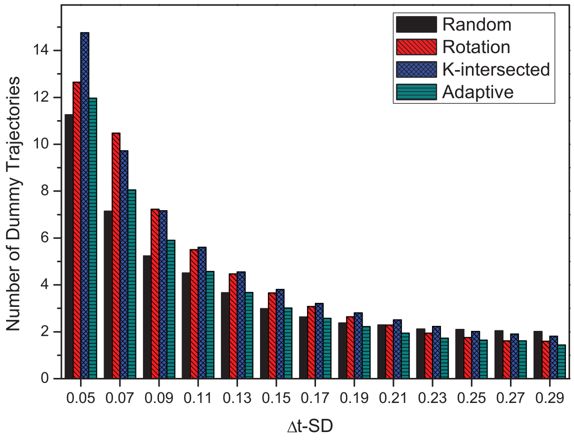


Figure 1. Influence of Δt-SD to the number of dummy trajectories

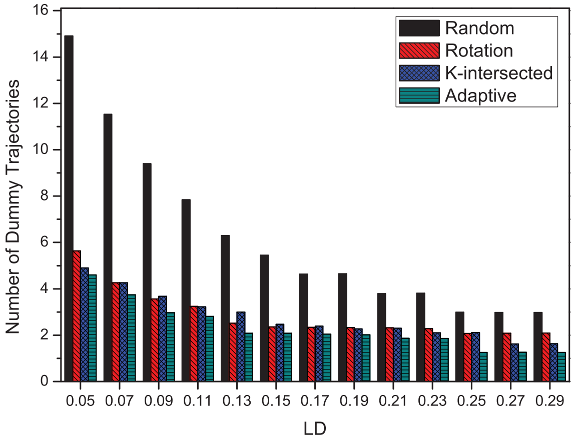


Figure 2. Influence of LD to the number of dummy trajectories

dummy trajectories satisfy TDD metric marked as *TDD* (line 4-7). Next, we discuss perturbation procedure (line 10). In the procedure, we select $(|T| * k)$ locations randomly, where $|T|$ is the number of locations in trajectory, k is the degree of perturbation. Then we move every location of $(|T| * k)$ in the direction where there are fewer locations. After moving, the new locations should not overlap with locations of other trajectories at the same time slot and the dummy trajectory should also fulfill the privacy metric *TDD*. Otherwise, the dummy trajectory will get back to the situation before the perturbation procedure. After perturbation we append the dummy trajectory to *Candidate* (line 11). The metrics Δt-SD and LD of every trajectory in candidate will be computed in the line 15, and the trajectory that has the smallest metrics will become a new dummy trajectory appended to *Dummies* (line 17). Repeat this procedure until dummy trajectories and the real trajectory can satisfy the Δt-SD and LD given by user (line 19). Finally, a dummy trajectory set *Dummies* is generated.

V. Experiments and Evaluation

In this section, we introduce the experiments conducted to evaluate privacy model and dummies generation algorithms. Firstly, the general situation of our experiment is presented and then we show the experiment results and analysis.

A. Experiment Introduction

We use the dataset that mobile devices connecting to campus net in USTC (University of Science and Technology of China) via Wi-Fi. In preprocessing, the trajectories of 100 devices in three months (from Sep. 1, 2013 to Nov. 30, 2013) are derived randomly as the experiments data. According to our proposed privacy model and algorithm, we conduct experiment using the trajectory of every user in each day, and then generating dummy trajectories. We statistics the outcomes conducted by all the real trajectories, and get the average of the outcomes.

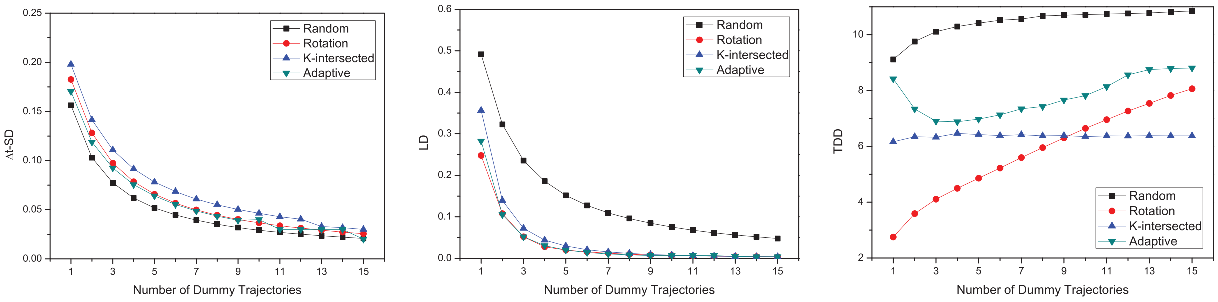
Specially, the map consists of equivalent grid cells, and the location of trajectory is marked by coordinate like (x, y). To emphasize ADTGA can generate less dummy trajectories than previous algorithms while it still fulfill the same level of privacy-preserving requirements, we implement the prior scheme algorithms in papers [2], [3] and compare them with our algorithm. The results and analysis of experiments will be described in the next section.

B. Results and Evaluation

In section V-B1, we investigate the correlation between the number of dummy trajectories and privacy metrics in privacy model. Then in the next section V-B2, we study the degree of privacy-preserving when algorithms generate the same number of dummy trajectories. We also investigate how the performance of adaptive dummy trajectories generation algorithm is affected by the various degree of perturbation which is presented in section V-B3.

*1) **Influence of metrics in privacy model to the number of dummy trajectories**:* In the procedure of generating dummy trajectories, when dummy trajectories have not satisfied the privacy-preserving requirements, additional dummy trajectories are included. However, a large amount of dummy trajectories increases the query message length, which leads to a heavy load on communication. Thus, one should generate as few dummy trajectories as possible to fulfill privacy requirements.

We first investigate the influence of Δt-SD to the number of dummy trajectories, and the result is showed in Fig 1. Suppose the other metrics are set to $LD = 0.4, TDD = 3, k = 2$ where the k is the intersections amount in the k-intersected algorithm, and adaptive degree of ADTGA is set to 0.5. As shown in result, all the algorithms generate fewer dummy trajectories with the increase of Δt-SD. In addition, due to randomly determining dummy locations in random scheme, the new trajectory is less likely to overlap with the trajectories that have generated. Therefore, the value of



(a) Δt-SD (b) LD (c) TDD

Figure 3. Influence of the number of dummy trajectories to privacy metrics

Δt-SD will be smaller, and fewer dummy trajectories are needed. Benefiting from perturbation procedure, ADTGA achieves almost the same number of dummy trajectories with random scheme, and fewer than rotation and k-intersected algorithm.

Next, Fig 2 shows the impact of LD. Suppose the other metrics are set to $\Delta t\text{-}SD = 0.4, TDD = 3, k = 2$, and adaptive degree of ADTGA is set to 0.5. Rotation, k-intersected and adaptive algorithm use a much smaller number of dummy trajectories to meet the LD requirement than random scheme does. By intersecting with other trajectories, the three better algorithms are able to increase the number of possible trajectories. Thus, they only need fewer dummy trajectories than the random to meet the requirements.

As shown in these experiments, all the algorithms can achieve the strict requirements. The probabilities of identifying real locations and trajectories by attackers are able to achieve 5%. Our algorithm ADTGA generates the almost same number of dummy trajectories with random scheme algorithm which is the best on Δt-SD. And about LD, adaptive algorithm has much smaller number of dummy trajectories than random scheme and that a little smaller than other two algorithms. Therefore, the adaptive uses fewer dummy trajectories to meet the same privacy requirements than previous algorithms.

*2) **Influence of the number of dummy trajectories to metrics in privacy model**:* For the purpose of studying the influence of the number of dummy trajectories to privacy metrics, in this section we generate the same number of dummy trajectories in all the algorithms, and observe the privacy-preserving requirements they can meet. Suppose the other metrics are set to $\Delta t\text{-}SD = 0.4, LD = 0.4, TDD = 2, k = 2$, and adaptive degree of ADTGA is set to 0.5.

Firstly, we investigate the influence to the Δt-SD which is shown in Fig 3(a). The random scheme algorithm can achieve the best Δt-SD among the four ones. Our adaptive algorithm is the second best algorithm in this experiment whose result is almost the same with that of the best one.

Secondly, the results on the LD are shown in Fig 3(b). Obviously the LD of trajectories generated by all the algorithm decreases when the number of dummy trajectories increases. The rotation, k-intersected and adaptive algorithm have nearly LD with the same number of dummy trajectories. However, the random scheme has a bad result on LD.

Finally, we study the impact of the number of dummy trajectories to TDD. TDD should be large enough to ensure dummy trajectories distributed uniformly, otherwise trajectories will be too close. As shown in Fig 3(c), random scheme algorithm can achieve the largest TDD when given the same number of dummy trajectories. Due to the perturbation procedure of ADTGA, it can also achieve a better TDD than rotation and k-intersected algorithm. Thus, dummy trajectories generated by ADTGA are distributed more uniformly than that by rotation and k-intersected algorithm.

In summary, under the condition that generating the same number of dummy trajectories, random scheme algorithm has a perfect performance on Δt-SD and TDD, but it gets an extremely bad result on LD. Although our adaptive algorithm is not good enough with random scheme on Δt-SD and TDD, it has a much better performance on the LD than random scheme. What's more, adaptive algorithm also performs better than rotation and k-intersected algorithm on all the metrics. Therefore, when there is the same number of dummy trajectories, our adaptive algorithm can satisfy stricter privacy-preserving requirements.

*3) **Influence of degree of perturbation to the number of dummy trajectories**:* In our proposed ADTGA, degree of perturbation is a variety that can affect the performance of the algorithm. Consequently, we conduct the experiment to observe the number of dummy trajectories on the same privacy requirements when the algorithm has different degrees of perturbation. We suppose the privacy requirements are set to $\Delta t\text{-}SD = 0.4, LD = 0.4, TDD = 2$, and the performance is shown in Fig 4.

The larger degree, the dummy trajectories generated can be more widely distributed, but are less likely to overlap with other trajectories. In this condition, there are more dummy trajectories needed to fulfill the LD. Thus, too large degree leads to a large number of dummy trajectories. On the contrary, the less degree of perturbation, the new dummy

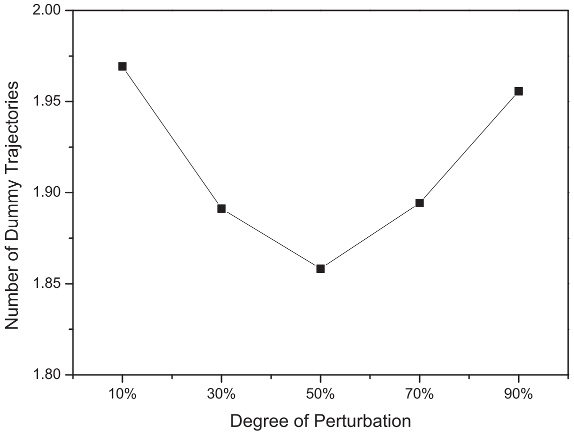


Figure 4. Influence of degree of perturbation to the number of dummy trajectories

trajectory is more likely to intersect other trajectories, but it is hard to satisfy Δt-SD. Therefore too large degree or too little degree leads to a large number of dummy trajectories, and the degree around 50% is the best.

VI. Conclusion and Future Work

To some extent, previous dummy trajectories generation approaches can preserve user real trajectory from being exposed to attackers in the long run. But there are still many problems such as unreasonable privacy metrics and too many dummy trajectories generated. To deal with these problems, we propose a new privacy model, and a new algorithm, which considers the influence of historical trajectories and includes a perturbation procedure. The performance analysis shows that dummy trajectories generated by our adaptive algorithm can satisfy stricter privacy-preserving requirements and the dummy trajectories can be distributed more uniformly on the map than existing algorithm.

Further investigations could be directed on two points. First, we intend to investigate reducing communication costs between user device and LBS provider on our approach. The dummy-based mechanism should not prevent smooth communication, otherwise, no users or LBS providers would use this approach. Second, it is possible to extend our approach to real environment, which could make dummy trajectories behave more naturally and enhance the capacity to protect user location privacy.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No.61033009, No.61303047 and No.61103228).

References

[1] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on.* IEEE, 2005, Conference Proceedings, pp. 88–97.

[2] T. H. You, W. C. Peng, and W. C. Lee, "Protecting moving trajectories with dummies," in *Mobile Data Management, 2007 International Conference on.* IEEE, 2007, Conference Proceedings, pp. 278–282.

[3] P. R. Lei, W. C. Peng, I. J. Su, and C. P. Chang, "Dummy-based schemes for protecting movement trajectories," *Journal of Information Science and Engineering*, vol. 28, no. 2, pp. 335–350, 2012.

[4] C. Y. Chow and M. F. Mokbel, *Enabling private continuous queries for revealed user locations.* Springer, 2007, pp. 258–275.

[5] X. Pan, J. L. Xu, and X. F. Meng, "Protecting location privacy against location-dependent attacks in mobile services," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 24, no. 8, pp. 1506–1519, 2012.

[6] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.* IEEE, 2008, Conference Proceedings.

[7] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Pervasive Computing and Communications Workshops, IEEE International Conference on.* IEEE Computer Society, 2004, Conference Proceedings, pp. 127–127.

[8] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in *Data Engineering (ICDE), 2011 IEEE 27th International Conference on.* IEEE, 2011, Conference Proceedings, pp. 494–505.

[9] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, 2003.

[10] A. Suzuki, M. Iwata, Y. Arase, T. Hara, X. Xie, and S. Nishio, "A user location anonymization method for location based services in a real environment," in *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems.* ACM, 2010, Conference Proceedings, pp. 398–401.

[11] R. Kato, M. Iwata, T. Hara, A. Suzuki, X. Xie, Y. Arase, and S. Nishio, "A dummy-based anonymization method based on user trajectory with pauses," in *Proceedings of the 20th International Conference on Advances in Geographic Information Systems.* ACM, 2012, Conference Proceedings, pp. 249–258.

[12] R. Kato, M. Iwata, T. Hara, Y. Arase, X. Xie, and S. Nishio, "User location anonymization method for wide distribution of dummies," in *Database and Expert Systems Applications.* Springer, 2013, Conference Proceedings, pp. 259–273.

[13] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: privacy-area aware, dummy-based location privacy in mobile services," in *Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access.* ACM, 2008, Conference Proceedings, pp. 16–23.