electronics

MDPI

Article

Trajectory Protection Schemes Based on a Gravity Mobility Model in IoT

Qiong Wu [1,2,3,*], Hanxu Liu [1], Cui Zhang [4,*], Qiang Fan [5], Zhengquan Li [1,2] and Kan Wang [6]

1 Jiangsu Provincial Engineering Laboratory for Pattern Recognition and Computational Intelligence, Jiangnan University, Wuxi 214122, China; hanxuliu@stu.jiangnan.edu.cn (H.L.); lzq722@jiangnan.edu.cn (Z.L.)
2 National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
3 Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
4 Huawei Technologies Co., Ltd, Shanghai 201206, China
5 Advanced Networking Lab., Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA; qf4@njit.edu
6 Faculty of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China; wangkan@xaut.edu.cn
* Correspondence: qiongwu@jiangnan.edu.cn (Q.W.); zhangcui3@huawei.com (C.Z.); Tel.: +86-510-8591-0633 (Q.W.); +86-21-5099-1818 (C.Z.)

Received: 10 December 2018; Accepted: 28 January 2019; Published: 31 January 2019

Abstract: With the proliferation of the Internet-of-Things (IoT), the users' trajectory data containing privacy information in the IoT systems are easily exposed to the adversaries in continuous location-based services (LBSs) and trajectory publication. Existing trajectory protection schemes generate dummy trajectories without considering the user mobility pattern accurately. This would cause that the adversaries can easily exclude the dummy trajectories according to the obtained geographic feature information. In this paper, the continuous location entropy and the trajectory entropy are defined based on the gravity mobility model to measure the level of trajectory protection. Then, two trajectory protection schemes are proposed based on the defined entropy metrics to protect the trajectory data in continuous LBSs and trajectory publication, respectively. Experimental results demonstrate that the proposed schemes have a higher level than the enhanced dummy-location selection (enhance-DLS) scheme and the random scheme.

Keywords: trajectory protection; entropy; gravity model; IoT

1. Introduction

Internet-of-Things (IoT) has great potential to be employed in various fields, including industrial controlling, automatic driving, environmental monitoring, and medical protection, which play a key role in supporting future smart cities [1,2]. This rapid proliferation of IoT has attracted numerous adversaries who attempt to capture the users' privacy information through exploiting IoT devices and eavesdropping the channel [3–8]. Hence, IoT attacks may incur serious sensitive privacy leakage and security issues; this is a potentially fatal threat to the long-term development of the IoT.

In IoT systems, a large number of sensors have been deployed for perception and information collection, which generate a huge amount of data. Such data consist of a lot of information on user trajectory. Once the adversaries acquire the users' trajectory data, they can analyze the users' trajectories to extract the users' sensitive information including home address, company address, health conditions, personal interests, and hobbies through data mining [9]. As a result, the adversaries can judge the uses' regular lifestyle and may make some harassment or behavior for the purpose of profit [10]. Therefore, the trajectory protection for IoT is especially a critical issue that urgently needs to be solved.

The user trajectory data in the IoT systems are exposed to the adversaries in two main ways. One is the continuous location-based services (LBSs), and the other one is the trajectory publication. The continuous LBSs can provide facilitated services to the mobile users and has been an essential component in their daily lives (e.g., navigation, location-based mobile advertising and requesting the nearest points of interests (PoIs) while traveling [11]). For the continuous LBSs, the users periodically send their real-time location obtained through a global positioning system (GPS) to the location service provider (LSP) to acquire the continuous service and thus, the users implicitly reveal their real-time location to the LSP which may be monitored by adversaries. In this case, users' historical trajectories may be collected by an untrustworthy LSP. On the other hand, for the trajectory publication, the LSP can further publish the collected historical trajectories to the third parties for data analysis. For example, the governors analyze the historical trajectories to predict the traffic congestion and further optimize the transport facilities [12]. Similarly, research institutes can analyze the historical trajectories to study human behavior patterns [13]. As a result, user trajectories are revealed to the third parties which may be monitored by adversaries in the trajectory publication. For simplification, adversary refers to both the untrustworthy LSPs and third parties in this paper.

In the past few years, many protection schemes have been proposed to protect the trajectories for continuous LBS or the trajectory publication [14–27]. The data of a trajectory is composed of a location dataset which includes a series of locations in chronological order, thus, the trajectory protection means protecting the chronological location data. The trajectory protection process of the continuous LBS is online since users' real-time locations need to be protected, while the trajectory protection process is performed offline for the trajectory publication. Most of the trajectory protection schemes are based on the k-anonymity method. The online k-anonymity-based trajectory protection scheme first generates $k-1$ dummy locations for a real-time location and then publishes the k locations that are composed of both $k-1$ dummy locations and a real-time location to confuse the adversaries, and thus, the real-time location of a trajectory can be protected. On the other hand, the offline k-anonymity-based trajectory protection scheme first generates dummy locations for each chronological location, then combines the dummy locations to generate $k-1$ dummy trajectories, and finally publishes k trajectories including the $k-1$ dummy trajectories and a real trajectory to protect the real trajectory.

In the real world, the adversaries can easily obtain the map information from the Internet, thus, they can easily exclude the dummy locations according to the geographic feature of the area that the dummy locations belong to. For example, if the adversaries have captured a location of a user and know the area around the user is a lake, thus, they can derive that the captured location is a dummy location. Therefore, some related works divide the region into different areas according to the geographic feature to generate the dummy location with high privacy level [14,28]. In [28], Niu et al. proposed an online k-anonymity-based trajectory protection scheme, i.e., enhanced dummy-location selection (enhance-DLS). In this scheme, the region is divided into different areas according to the geographic feature. They used entropy metric to measure the privacy level between different areas. The entropy is calculated according to the query probability and the transition probability. The query probability is the probability that a user launches a query in an area and the transition probability is the probability that a user moves from an area to another. However, the DLS scheme assigned the transition probability randomly without considering the realistic user mobility pattern. The user mobility pattern reflects the commuting flow for a user from one area to another. If the user mobility pattern is not considered to generate dummy trajectories, the adversaries can easily exclude the dummy trajectories according to the obtained geographic feature information. For example, a user utilizes a 2-anonymity scheme to protect the real-time location as shown in Figure 1. We denote ru_t as the real user's location at moment t, and du_t is the dummy location of the user at moment t. For $t = 1$ and $t = 2$, the scheme generates 1 dummy location respectively. If the adversaries has learned that there is a lake between ru_1 and du_2, du_1 and ru_2, du_1 and du_2, thus, they can easily exclude the dummy trajectories $ru_1 \rightarrow du_2$, $du_1 \rightarrow ru_2$ and $du_1 \rightarrow du_2$. As a result, the adversaries can successfully derive the real trajectory $ru_1 \rightarrow ru_2$ by inference. Therefore, the user mobility pattern is an important factor which

should be considered to calculate the user commuting flow and further obtain accurate transition probability between two areas, thus, creating dummy locations with a high privacy level.

Some user mobility models have been established for trajectory privacy protection. Bindschaedler et al. employed the Markov model to characterize human mobility pattern, but this model is not suitable for long-term processing of data and has high computational complexity [15]. Lei et al. proposed dummy generation schemes based on random pattern and intersection pattern, while their mobility model can only be used for users with consistent movement patterns [16]. Another popular user mobility model is the gravity model. The gravity model derived from Newton's law of universal gravitation, which are widely used in transportation theory [29,30]. It shows that the commute flow between the two regions is proportional to theirs flow scale, and inversely proportional to their distance. The gravity model can describe the interactions between different geographical areas of the city, such as pedestrian commute flow, traffic flow and the flow of calls or messages [31]. In [32], Jung et al. studied the case of the road network and concluded that the interaction strength also follows the gravity model. Different from other user mobility models, the gravity model has been proven to be a suitable method to depict human mobility patterns, and has been widely employed in mobility analysis for transportation, population migration and geographic information prediction [33–35]. To the best of our knowledge, no works have considered the gravity model to obtain the transition probability in the existing trajectory protection schemes. This motivated us to conduct this work.

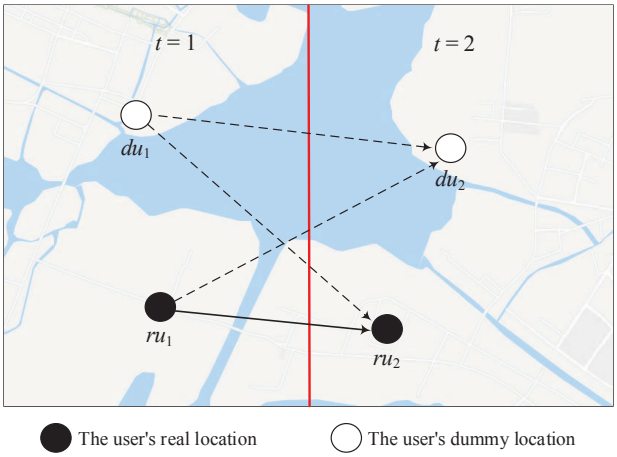

Figure 1. An illustration of dummies generation based on 2-anonymity.

In this paper, we propose two *k*-anonymity-based trajectory protection schemes considering the user mobility pattern to protect the trajectory data in continuous LBSs and trajectory publication, respectively. In the schemes, dummy trajectories are created according to the continuous location entropy and the trajectory entropy that are defined to measure the privacy level of trajectories. Our contributions are summarized as follows:

- We propose two *k*-anonymity-based trajectory protection schemes considering the mobility pattern to protect the trajectory data in continuous LBSs and trajectory publication, respectively.
- We define the continuous location entropy and trajectory entropy to measure the privacy level of the dummy trajectory. The gravity model is adopted to evaluate user commuting flow and further obtain accurate transition probability of the defined entropies.
- We conduct comprehensive experiments to demonstrate that our proposed schemes can achieve better performance as compared to other methods.

The rest of the paper is organized as follows. Section 2 introduces related work. The system model is described in Section 3. We propose trajectory protection schemes in continuous LBS and trajectory publication in Section 4. In Section 5, the detailed experiment is shown. Section 6 concludes the paper.

2. Related Work

In this section, we mainly review the existing trajectory protection schemes in continuous LBS and trajectory publication. In addition, we introduce some related works on user mobility pattern in the past few years.

We first review the related trajectory protection schemes in continuous LBS. To protect the trajectory data in the continuous LBS, Kido et al. [14] proposed two dummy trajectory generation algorithms that generate dummies without relying on the third party. The next dummy location is determined according to the users' neighborhood location. The algorithms employ a random walk model to generate dummy locations without considering the user movement pattern. Xu et al. [17] proposed a k-anonymity-based trajectory protection scheme that employs other users' historical trajectories to generate dummy trajectories. It ensures the authenticity and validity of the other $k-1$ dummy trajectories, which makes it harder for adversaries to infer the real users' trajectories when the mobile user launches continuous LBSs during his movement. However, due to the query probability and the transition probability not being fully considered, the adversary can infer the user's real trajectory with a large probability.

Xu and Cai [18] defined a spatial region as 2^E, where E is the location entropy. The location entropy is used to measure the popularity of the region based on footprints collected from the visitors of the region. The cloaking algorithms depend on an anonymizer server. Wu et al. [19] proposed a k-anonymity dummy trajectory generation method based on client-side. It constructs the set of dummy trajectories by adjusting the angle between the dummy trajectories and the real trajectory, thus, avoiding the coincidence of the dummy trajectories and the real trajectory. Lei et al. [16] obtained the dummy trajectories by rotating the real trajectory generated by the user, so that the adversary could not identify the real trajectory with the knowledge of the geometric shape and direction of the trajectory. Moreover, they only consider a user's profile after a long-term observation but not protect the trajectory data in real time. In order to resist inference attacks, Niu et al. [20] proposed an efficient trajectory protection scheme called DUMMY-T, which aims to protect the user's trajectory against adversaries with the obtained information in the continuous LBS. They generate the dummy locations with minimum cloaking region while ignore the user's real movement pattern. Bindschaedler et al. [15] designed a privacy-preserving generative model to synthesize the trajectories of some individuals with consistent lifestyles. They concentrated on the mobility similarity metric and ensured the tradeoff between location privacy and utility. Kini et al. [21] considered a k-anonymity-based location generation algorithm that takes into account the data characteristics in real world and implemented the algorithm in realistic mobility scenarios, but the authors studied the complexity and communication overhead of the algorithm without discussing the effect of privacy protection. Peng et al. [22] proposed an enhanced location privacy preserving (ELPP) scheme that doesn't require fully trusted entity. Instead, an entity named function generator is introduced. The function generator exploits the Hilbert curve to convert a real location into a dummy location to achieve the trajectory protection. However, this method is not able to accurately depict the similarity between the real and the dummy trajectories. As mentioned above, the related trajectory protection schemes in continuous LBS have not considered the user movement pattern.

Next, we review the related works about the existing trajectory protection schemes in trajectory publication. Terrovitis and Mamoulis [23] studied the problem of privacy preservation in the trajectory publication. They hold the view that if trajectories are published exactly, the risk of privacy exposure will be increased. Therefore, they proposed a data suppression technique that suppresses the exposure of trajectory database. However, if more trajectory dataset are suppressed, the trajectory data would be lost and become worthless. Chen et al. [24] protected the published trajectory data based on a differential privacy model. They proposed an efficient data-dependent privacy sanitization algorithm, the algorithm remains high utility and is available to protect large trajectory datasets. Abul et al. [25] presented the concept of (k, δ)-anonymity for protecting trajectory data publication, here δ represents the possible of the location imprecision. The authors modified the trajectories through space translation

technique, then k different trajectories can exist in a cylinder with radius δ. Pensa et al. [26] proposed a new k-anonymity-based approach to preserve the sequential data in the field of knowledge discovery and mobility data mining. They converted the sequential data to another one by means of insertions, deletions or substitutions. Nergiz et al. [27] proposed a randomization-based reconstruction algorithm for protecting the disclosed trajectory data by extending the notion of k-anonymity. From the related works mentioned above, we can see that there are no relevant trajectory protection schemes that consider the user mobility pattern in trajectory data publication.

After that, we review some works which used the gravity model to describe the human movement pattern between different regions. Krings et al. [33] investigated the communications flows for inter-city and described the communication intensity by a gravity model. In [34], Tomita et al. used the gravity model to present a quantitative analysis about migration, which shows precise predictions about movement of population. To the best of our knowledge, no works have considered the gravity model to obtain the transition probability and further generated the dummy trajectories in the k-anonymity-based trajectory protection schemes. This motivated us to conduct this work. Wang et al. [36] proposed a hybrid predictive model that applies the gravity model to depict both the regularity and conformity of human mobility as well as their mutual reinforcement. However, there are no works on trajectory protection schemes that use the gravity model to depict the user mobility patterns.

Conclusively, the existing trajectory protection schemes in both continuous LBS and trajectory publication have not considered the user mobility pattern to generate dummies. The gravity model can depict the user mobility patterns. In our schemes, we will employ the gravity model to calculate the transition probability and further generate dummies with high privacy level.

3. System Model

In this section, we introduce the system model of this paper. We consider protecting the users' trajectory data of the continuous LBS and the trajectory publications in a region. A trajectory data is a location dataset with a series of chronological location data. Thus, protecting the trajectory data means protecting the chronological location data. As in [28], we divide the region into $l \times l$ girds with equal sizes according to the geographic feature of the region and label these grids in order.

The users, LSPs, third parties and the base station are distributed in the region as shown in Figure 2. The LSPs usually refer to the servers of the large companies, e.g., Google and Baidu. The LSPs can provision location based services to users through communication network [37–40]. The LSPs store the users' historical trajectory data in a storage module while provisioning the continuous LBSs to the users. The users move in the region according to the human daily activities. Each user is equipped with a mobile device. The mobile device is usually storable and computable, which receives the location-based service (such as smartphones, tablet personal computers and wearable devices). The mobile device can obtain the historical trajectory data of the users in the region from the LSP and store the trajectory data in a storage module. The trajectory data stored in the storage module is updated in each time period. Each mobile device and the LSP have a gravity model module, which can construct the corresponding gravity model based on the stored historical trajectory data. Moreover, each mobile device and the LSP also have a dummy-fuse module to generate dummy location data. The dummy-fuse module calculates the query probabilities of the grids in the region according to the historical trajectory data in the storage module, and uses the gravity model constructed in the gravity model module to calculate the transition probabilities between different grids in the region. Then, the calculated query probabilities and the transition probabilities are stored in the dummy-fuse module.

Next, we introduce the continuous LBS process and the trajectory publication process in the system model. The continuous LBS process is first described. In the continuous LBSs, we assume that the LSP is an active adversary which obtains the privacy information of users, e.g., history visiting records. Each user in the region launches a query to the LSP to obtain a service periodically. For each query, the mobile device of the user first obtains their real-time location data from the GPS before launching a query and stores the real-time location data. Then, the dummy-fuse module in the mobile

device generates $k-1$ dummy locations with high privacy metric and fuses them with the real-time location data. This process is the trajectory protection process of the continuous LBS. Afterwards, with the fused k location data, the user sends them to the LSP through the communication networks to protect the real-time location data. Finally, the LSP records the k location data and returns the corresponding service to the user. After the continuous LBS process is completed, the LSP records the user's trajectory data. Therefore, the LSP usually record large amounts of the users' trajectory data which can be published to the third party for analysis. Next, the trajectory publication process is introduced. In the trajectory publication, we assume the third party is the adversary. To protect the trajectory data, the dummy module in the LSP generates $k-1$ dummy trajectories with high privacy metric and fuses them with the real trajectory data. This process is the trajectory protection process of the trajectory publication. The continuous LBS and the trajectory publication process in the system model is shown in Figure 3. As mentioned above, the trajectory protection process of the continuous LBS and trajectory publication are both conducted to protect the trajectory data. The former process is conducted to protect the on-line location data in the continuous LBS while the latter process is conducted to protect the off-line trajectory data in the trajectory publication.

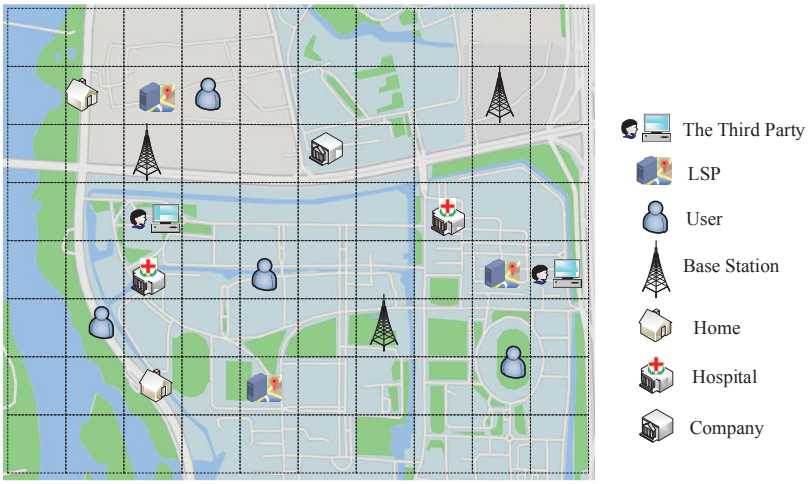

Figure 2. The region considering in the system model.

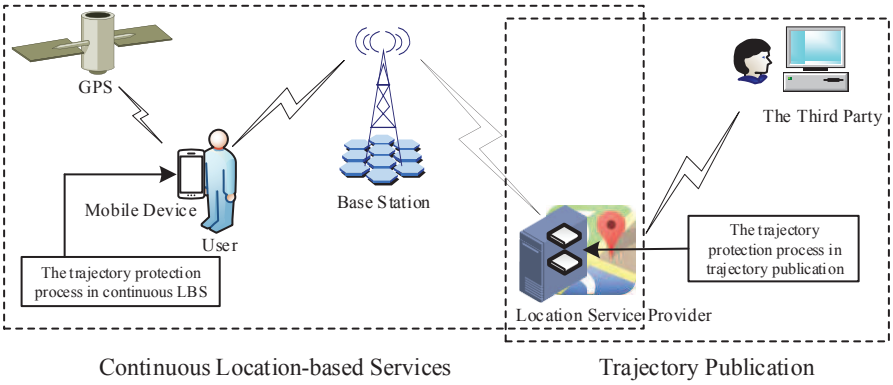

Figure 3. The continuous LBSs process and the trajectory publication process in the system model.

Then, we will introduce the trajectory protection process of the continuous LBS and trajectory publication. The two trajectory protection processes are conducted in eight steps. The steps are shown as follows,

(1) The historical data are obtained from the storage module.
(2) The query probability is calculated through historical data.
(3) The gravity model is fitted based on historical data.

(4) The transition probability between the two locations can be predicted according to the gravity model.

(5) The candidates of dummy locations are selected. This step is different for the continuous LBS and trajectory publication process. In continuous LBS, the user's maximum movement limit is determined according to the user's maximum velocity and the interval between two continuous queries. Afterwards, the number of dummy location candidates within the maximum movement limit are determined. However, in trajectory publication, the trajectory is first decomposed into a number of locations, then the candidates are determined based on the maximum movement limit of each location in the trajectory.

(6) The entropy metric is calculated according to the query probability and the transition probability. The continuous location entropy is calculated according to the probabilities between two locations for continuous LBS while the trajectory entropy is calculated according to the probabilities among the locations in a trajectory for trajectory publication.

(7) The dummies are obtained based on the corresponding entropy metric. In continuous LBS, the $k-1$ locations corresponding to the optimal continuous location entropy is selected. On the other hand, the $k-1$ location combinations corresponding to the optimal trajectory entropy is obtained.

(8) The k trajectory data are generated through fusing the $k-1$ dummy data with the real data. Then the fused k trajectory data are obtained. The user sends them to the LSP in continuous LBS, or the LSP sends to the third party in trajectory publication.

The flowchart of these two trajectory protection processes in continuous LBS and trajectory publication is shown in Figure 4.

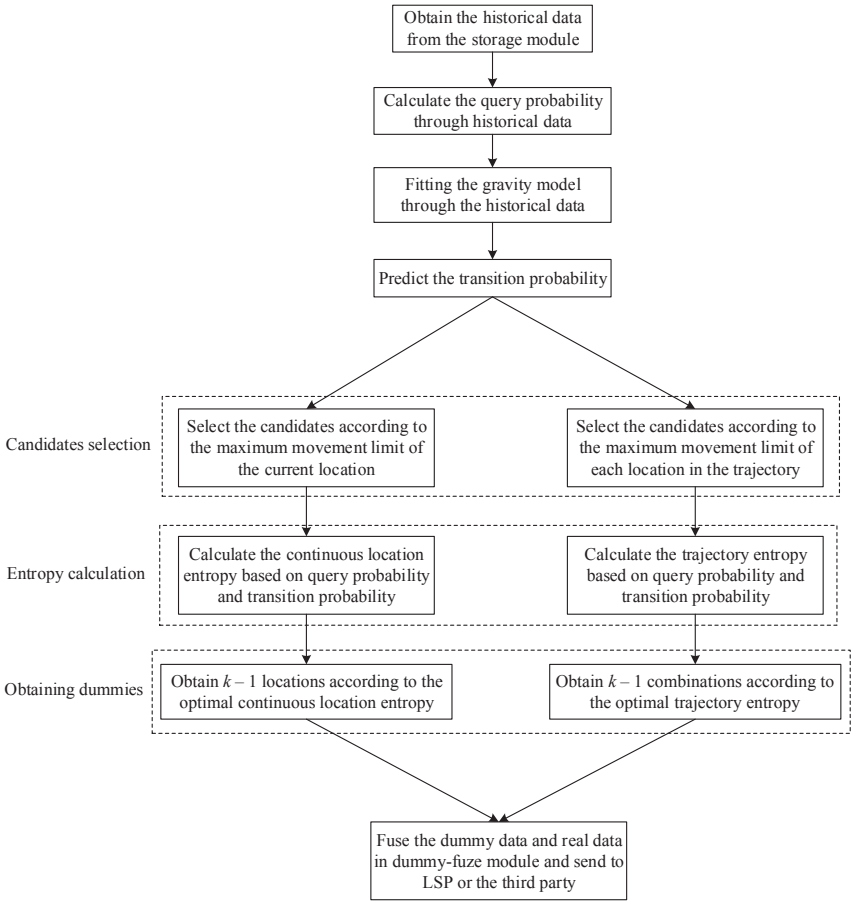

Figure 4. The flowchart of trajectory protection process in continuous LBS and trajectory publication.

4. Trajectory Privacy Protection Schemes

In this section, we introduce our proposed k-anonymity-based schemes to generate dummy trajectories in the continuous LBS and the trajectory publication, respectively. We define the continuous location entropy for the continuous LBS and the trajectory entropy to measure the privacy level of the dummy trajectories. In order to reflect the real user mobility pattern, the transition probability in the continuous location entropy and the trajectory entropy is calculated according to the gravity model. The proposed schemes generate dummy trajectories by selecting the trajectories with high privacy level. In this section, we first introduce the continuous location entropy and the trajectory entropy. Afterwards, we will further describe the proposed schemes in detail.

4.1. Continuous Location Entropy and Trajectory Entropy

In this section, we firstly introduce the concept and meaning of entropy. Entropy derived from the Shannon's theory of information. According to the Jaynes' maximum entropy principle, we learned that Shannon entropy can be used to measure the privacy of confidential data according to the probability distribution [41]. In [42], the authors mentioned that entropy can be used to measure the anonymity of the user's behaviors. Inspired by this principle, we define the continuous location entropy and the trajectory entropy as the performance metric to quantize the privacy level of the trajectory in the continuous LBSs and the trajectory publication, respectively. The continuous location entropy and the trajectory entropy are novel concepts derived from location entropy [27,36].

Let $X_j(j = 1, 2, \cdots, k)$ be the jth trajectory of the generated k trajectories. Assuming the length of a trajectory is m, the trajectory X_j with the location data generated at moments $t_1, t_2, \cdots, t_i, \cdots, t_m$, $(i = 1, 2, \cdots, m)$ can be denoted as $X_j = \{x_j^1 \rightarrow x_j^2 \rightarrow \cdots \rightarrow x_j^i \rightarrow \cdots \rightarrow x_j^m\}$, where x_j^i is the grid where the user is located at moment t_i on the jth trajectory.

For the trajectory from x_j^i to $x_j^{i'}$, let $P(x_j^i \rightarrow x_j^{i'})$ be the probability that the user moves from x_j^i to $x_j^{i'}$ and he launches query at each location from x_j^i to $x_j^{i'}$, $q(x_j^{h'})$ be the query probability that the user initiates a query at $x_j^{h'}$ $(i \leq h' \leq i')$, $p_t(x_j^{h-1} \rightarrow x_j^h)$ be the transition probability that the user moves from x_j^{h-1} to x_j^h $(i+1 \leq h \leq i')$, thus, $P(x_j^i \rightarrow x_j^{i'})$ can be calculated as

$$P(x_j^i \rightarrow x_j^{i'}) = \prod_{h'=i}^{i'} q(x_j^{h'}) \prod_{h=i+1}^{i'} p_t(x_j^{h-1} \rightarrow x_j^h), \tag{1}$$

According to the definition of the entropy [43], the entropy (i.e., the privacy level) of the k trajectories generated from moment t_i to moment t_i' is calculated as

$$HC_k(x^i, x^{i'}) = -\sum_{j=1}^{k} P(x_j^i \rightarrow x_j^{i'}) log_2(P(x_j^i \rightarrow x_j^{i'})) \tag{2}$$

In the continuous LBSs, regarding one real-time location, we assume that the $k-1$ dummy locations are generated accordingly at moment t_i. Hence, regarding the real-time trajectory, $k-1$ dummy trajectories are generated from moment t_{i-1} to t_i, $(i = 2, 3, \cdots, m)$. According to the Equations (1) and (2), the entropy of the k trajectories generated from t_{i-1} to t_i is calculated as

$$HC_k(x^{i-1}, x^i) = -\sum_{j=1}^{k} P(x_j^{i-1} \rightarrow x_j^i) log_2(P(x_j^{i-1} \rightarrow x_j^i)) \tag{3}$$

$$P(x_j^{i-1} \rightarrow x_j^i) = q(x_j^{i-1}) p_t(x_j^{i-1} \rightarrow x_j^i) q(x_j^i), \tag{4}$$

In this paper, we define the entropy $HC_k(x^{i-1}, x^i)$ in Equation (3) as the continuous location entropy to measure the privacy level of the trajectories generated in the continuous LBSs.

In the trajectory publication, $k-1$ dummy trajectories are generated from moment t_1 to t_m. Therefore, according to the Equations (1) and (2), the entropy of the k trajectories from t_1 to t_m is calculated as

$$HR_k(x^1, x^m) = -\sum_{j=1}^{k} P(x_j^1 \to x_j^m) log_2(P(x_j^1 \to x_j^m)) \tag{5}$$

$$P(x_j^1 \to x_j^m) = \prod_{i'=1}^{m} q(x_j^{i'}) \prod_{i=2}^{m} p_t(x_j^{i-1} \to x_j^i), \tag{6}$$

Similarly, we define the entropy $HR_k(x^1, x^m)$ in Equation (5) as the trajectory entropy to measure the privacy level of the trajectories generated in the trajectory publication.

To obtain the the continuous location entropy in Equation (3) and the trajectory entropy in Equation (5), we will further determine the query probability $q(x_j^i)$ and the transition probability $p_t(x_j^{i-1} \to x_j^i)$. Next, we will introduce how to derive the query probability $q(x_j^i)$ and the transition probability $p_t(x_j^{i-1} \to x_j^i)$.

4.1.1. Query Probability

In this section, we introduce how to obtain the query probability. Let a be a grid in the region. We use N to represent the number of grids. As described in Section 3, the mobile devices of users can store the historical trajectories in the region. Hence, they can obtain the number of user queries in each grid by analyzing the users' historical trajectories. Thus, the query probability $q(a)$ can be calculated as follows,

$$q(a) = \frac{Q(a)}{\sum_{g=1}^{N} Q(g)}, (g = 1, 2, \cdots, N), \tag{7}$$

where $Q(a)$ and $Q(g)$ indicates the number of user queries in grid a and g.

The query probability of each grid is stored in mobile devices after being calculated.

4.1.2. Transition Probability

In this section, we introduce how to obtain the transition probability. Let a and b be two grids in the region. The transition probability $p_t(a \to b)$ can be calculated by

$$p_t(a \to b) = \frac{F(a, b)}{\sum_{g \in N} F(a, g)}, (g = 1, 2, \cdots, N), \tag{8}$$

where $F(a, b)$ is the commuting flow from grid a to grid b and $F(a, g)$ is the commuting flow from grid a to grid g.

In order to reflect the real user mobility pattern, we employ the gravity model to predict the commuting flow from a grid to another grid. Since the gravity model integrates the regularity and conformity of human mobility as well as their mutual reinforcement, it is realized as a precise estimation of commuting flow which is widely applied in mobility analysis for a large population such as traffic, migration and trade flows [36]. According to the gravity model in [36], the communing flow $y_{m,n}$ from grid m to grid n is calculated according Equation (9),

$$y_{m,n} = \alpha \cdot \frac{(u_m)^{\mu} \cdot (v_n)^{\theta}}{\exp(\gamma \cdot w_{m,n})}. \tag{9}$$

In Equation (9), we denote u_m as the flow of the user leaving grid m, v_n as the flow of the user arriving at grid n, and $w_{m,n}$ as the distance between grid m and grid n. μ, θ, γ are the coefficients of the leaving flow, the arriving flow and the distance, respectively; α is the coefficient of the commuting flow. The coefficients μ, θ, γ and α are different for different people flows in different regions.

Taking a logarithm at the both sides of Equation (9), the commuting flow $y_{m,n}$ is a function of the coefficients μ, θ, γ and α as

$$\ln y_{m,n} = \ln \alpha + \mu \cdot \ln u_m + \theta \cdot \ln v_n - \gamma \cdot w_{m,n}, \tag{10}$$

In our paper, we use Equation (9) to predict the commuting flow from a grid to another grid. The historical trajectory data stored in mobile devices can approximately reflect the people flow in the grids of the region. For the grids of the region, let L_a be the flow of the user leaving gird a, A_b be the flow of the user arriving at grid b and $dist_{a,b}$ be the average distance between grid a and location b. $F(a,b)$, L_a, A_b and $dist_{a,b}$ can be obtained through observing the historical trajectory data stored in the mobile devices. Our objective is to obtain the coefficients μ, θ, γ and α which can enable the gravity model function, i.e., Equation (10), to fit the observed data in the grids of the region (i.e., including $F(a,b)$, L_a, A_b and $dist_{a,b}$). thus, the commuting flow of the area from a grid to another grid can be predicted through gravity model function with the obtained coefficients μ, θ, γ and α. Since the gravity model function can be transferred to be Equation (10), our objective can be equivalent to obtain the coefficients μ, θ, γ and $\ln \alpha$ to make Equation (10) fit the observed data in the grids of the region including $\ln F(a,b)$, $\ln L_a$, $\ln A_b$ and $dist_{a,b}$. The difference between $\ln F(a,b)$ and the predicted value of Equation (10) is denoted as $\epsilon_{a,b}$, thus, we have

$$\ln F(a,b) = \ln \alpha + \mu \cdot \ln L_a + \theta \cdot \ln A_b - \gamma \cdot dist_{a,b} + \epsilon_{a,b}. \tag{11}$$

In Equation (11), $F(a,b)$, L_a, A_b and $dist_{a,b}$ can be obtained through observing the historical trajectory data. For a trajectory, it consists of multiple locations. The leaving flow L_a can be obtained through counting the number of trajectories in which the current location is in grid a and the next location is out of grid a. The arrival flow A_b can be obtained through counting the number of trajectories in which the current location is out of grid b and the next location is in grid b. The average distance $dist_{a,b}$ between grid a and grid b can be obtained by calculating the distance between the center point of grid a and the center point of grid b. Meanwhile, the commuting flows $F(a,b)$ can be obtained through counting the number of trajectories from a location in grid a to the another location in grid b.

To facilitate the estimation of coefficients of Equation (11), Equation (11) is converted into the matrix form of standard multivariate linear regression equation shown as follows,

$$\boldsymbol{Y} = \boldsymbol{X}\boldsymbol{\beta} + \epsilon. \tag{12}$$

In Equation (12), we have $\boldsymbol{Y} = (Y_1, Y_2, \cdots, Y_{(a-1)N+b}, \cdots, Y_{N^2})^T$, where $Y_{(a-1)N+b} = F(a,b)$. $\boldsymbol{X}$ is the matrix shown as follows,

$$\boldsymbol{X} = \begin{pmatrix} 1 & X_{1,1} & X_{1,2} & X_{1,3} \\ 1 & X_{2,1} & X_{2,2} & X_{2,3} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & X_{(a-1)N+b,1} & X_{(a-1)N+b,2} & X_{(a-1)N+b,3} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & X_{N^2,1} & X_{N^2,2} & X_{N^2,3} \end{pmatrix}, \tag{13}$$

where $X_{(a-1)N+b,2} = \ln L_a$, $X_{(a-1)N+b,3} = \ln A_b$, $X_{(a-1)N+b,4} = dist_{a,b}$. The coefficient vector can be expressed as $\boldsymbol{\beta} = (\ln \alpha, \mu, \theta, -\gamma)^T$.

Considering that the random error $\boldsymbol{\epsilon}$ satisfies the normal distribution and is independently and identically distributed, we can use the least square method to estimate the coefficient vector $\boldsymbol{\beta}$. According to [44], the residual sum of squares is used to express the error between the observed value and the predicted value, i.e.,

$$SSE = \|\boldsymbol{X}\boldsymbol{\beta} - \boldsymbol{Y}\|^2. \tag{14}$$

According to the least square method [44], the coefficient vector $\hat{\boldsymbol{\beta}}$ which minimumises the residual sum of squares is calculated as

$$\hat{\boldsymbol{\beta}} = (\boldsymbol{X}^T\boldsymbol{X})^{-1}\boldsymbol{X}^T\boldsymbol{Y}. \tag{15}$$

Based on the above deduction, we can achieve the coefficients $\hat{\boldsymbol{\beta}}$ in the gravity model. When $\boldsymbol{\beta} = \hat{\boldsymbol{\beta}}$, the the residual sum of squares is minimum, i.e., the error between the observed value and the predicted value is minimum. Thus, $\hat{\boldsymbol{\beta}}$ are the optimal coefficients which enable the gravity model to fit the observed value. Therefore, the gravity model that depicts the user mobility pattern are obtain according to the stored trajectory data.

The commuting flows between different grids are calculated according to the obtained gravity model and the transition probabilities between different grids are calculated according to Equation (8). Then the transition probabilities are stored in mobile devices.

4.2. Trajectory Protection Schemes

In Section 4.1, we have introduced the continuous location entropy and the trajectory entropy to measure the privacy level of the dummy trajectory generated in the continuous LBS and trajectory publication, respectively. In this section, we will introduce the trajectory protection schemes that generate dummy trajectories according to the continuous location entropy and the trajectory entropy, respectively.

4.2.1. Trajectory Protection Schemes for the Continuous LBSs

In this section, we introduce the on-line trajectory protection scheme to protect the trajectory in the continuous LBSs. The on-line trajectory protection scheme protects the trajectory from t_1 to t_m by generating $k-1$ dummy locations in real time. At each moment, the trajectory protection scheme is conducted to generate $k-1$ dummy locations to protect the real-time location. Let $\{TD_1, TD_2, \cdots, TD_m\}$ be the grid sets where dummy locations are generated at moments $t_1, t_2, \cdots, t_m$. At t_1, the enhanced-DLS scheme is adopted to determine the location dataset, i.e., the k locations consisting of 1 real location and the $k-1$ dummy locations with undistinguishable geographic information [28], and thus, we get $TD_1 = \{x_1^1, x_2^1, \cdots, x_j^1, \cdots, x_k^1\}$, where x_j^1 means the grid where the jth dummy location is located at t_1. For moment t_2, the trajectory protection schemes for the continuous LBSs are described as follows. Let v_{max} be the user's maximum speed, Δt be the time interval between two continuous queries. Since the user's moving distance should not be larger than the maximum moving distance, i.e., $v_{max} * \Delta t$, the jth dummy location at t_2 should be generated within the circle around jth dummy location at t_1 with the radius $v_{max} * \Delta t$. To generate the dummy location, the grids within the circle are determined and the grid numbers $\{s_1, s_2, \cdots, s_{max}\}$ are stored. Then the query probabilities of the grids $\{s_1, s_2, \cdots, s_{max}\}$ and the transition probabilities from x_j^1 to the grids $\{s_1, s_2, \cdots, s_{max}\}$ are extracted from the mobile device to calculate the continuous location entropy from x_j^1 to each of the grids by Equations (3) and (4). The grid corresponding to the maximum continuous location entropy is selected as x_j^2 and the jth dummy location at moment t_2 is randomly selected from the grid x_j^2. Similarly, we will repeat the above procedure for each dummy location generated at moment t_1, thus, the $k-1$ dummy locations generated at moment t_2 are determined. Repeating dummy locations generation process for each moment, thus, the real-time location can be protected through generating $k-1$ dummy locations at each moment. The process of the on-line scheme is shown in Figure 5 and the detailed dummy location generation process in continuous LBSs is shown in Algorithm 1.

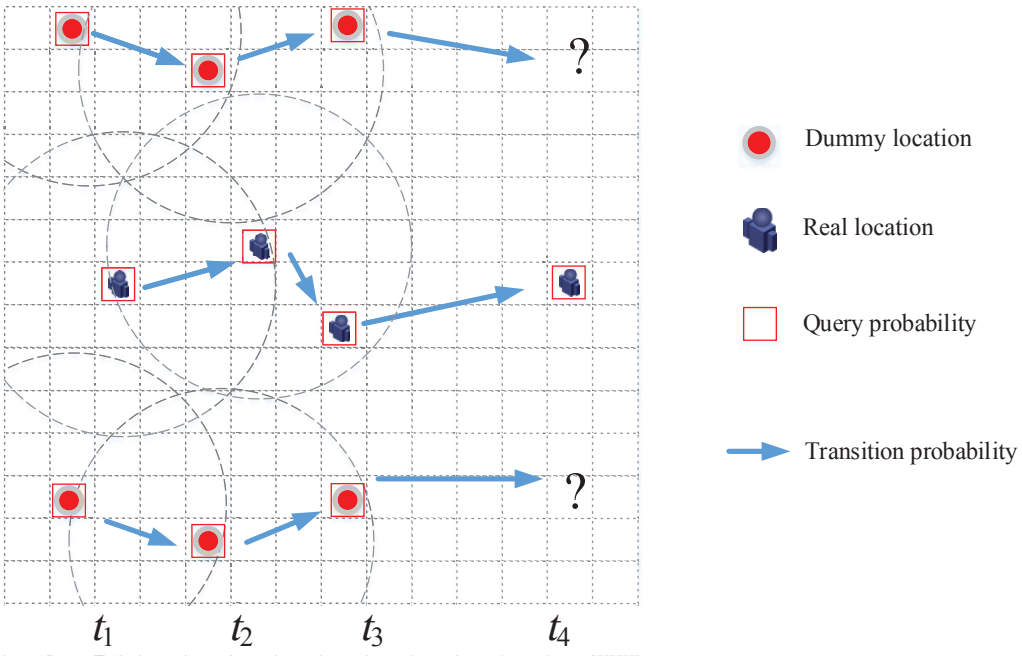

Figure 5. Dummy locations selection in continuous LBS.

Algorithm 1: Dummies Generation Algorithm in Continuous LBSs

for $(i = 2; i <= m; i++)$
{
  for $(j = 1; j <= k-1; j++)$
  {
    Determining all the grids filled in the circle at time t_{i-1} and obtaining the grid numbers $\{s_1, s_2, \cdots, s_r, \cdots, s_{max}\}$
    for $(s_r = s_1; s_r <= s_{max}; r++)$
      {
      Compute the continuous location entropy using
      $P(x_j^{i-1} \to s_r) = q(x_j^{i-1}) p_t(x_j^{i-1} \to s_r) q(s_r)$
      $H = -P(x_j^{i-1} \to s_r) log_2(P(x_j^{i-1} \to s_r))$
      }
    Selecting the grid s_r corresponding to maximum continuous location entropy
    Adding the grid to the dummy location dataset
  }
Outputing $k-1$ dummy locations
Fusing 1 real-time location data with $k-1$ dummy locations
}

4.2.2. Trajectory Protection Scheme in Trajectory Publication

In this section, we introduce the off-line trajectory protection scheme to protect the trajectory data in trajectory publication. The off-line trajectory protection scheme protects the trajectory by generating $k-1$ dummy trajectories.

The scheme is conducted before a user publishes his trajectory data $X = \{x_1 \to x_2 \to \cdots \to x_i \to \cdots \to x_m\}$. The process of the off-line scheme is described as follows. Firstly, according to the maximum moving distance $v_{max} * \Delta t$, the grid numbers within the circle of each x_i are determined as Algorithm 1. The number of grids in circle i is denoted as n_i. Then, for each time, a unique grid is chosen from each circle and combining these grids to be a grid combination. As a result, $\prod_{i=1}^{m} n_i$ different grid combinations can be obtained. Then, the trajectory entropies of all the combinations

are calculated according to Equations (5) and (6). Finally, the combinations with the $k-1$ maximum entropies are selected and $k-1$ dummy trajectories are generated by randomly selecting a location within each of the selected grids. The process of the off-line scheme is shown in Figure 6 and the detailed dummy trajectory generation process in trajectory publication is shown in Algorithm 2.

Algorithm 2: Dummy Trajectories Generation Algorithm in Trajectory Publication

1 Determining all the grids filled in the m circles, obtaining the number of grids in each circle $\{n_1, \cdots, n_m\}$
2 For each time, choosing a unique grid from the grids within each circle and connect them to obtain $\prod_{i=1}^{m} n_i$ different grid combinations
3 Computing the trajectory entropies for all the combinations using Equations (5) and (6)
4 Selecting $k-1$ grid combinations with the maximum trajectory entropies and selecting randomly a location within each of the selected grids to generate dummy $k-1$ trajectories
5 Output $k-1$ dummy trajectories
6 Fusing 1 real trajectory with $k-1$ optimal dummy trajectories

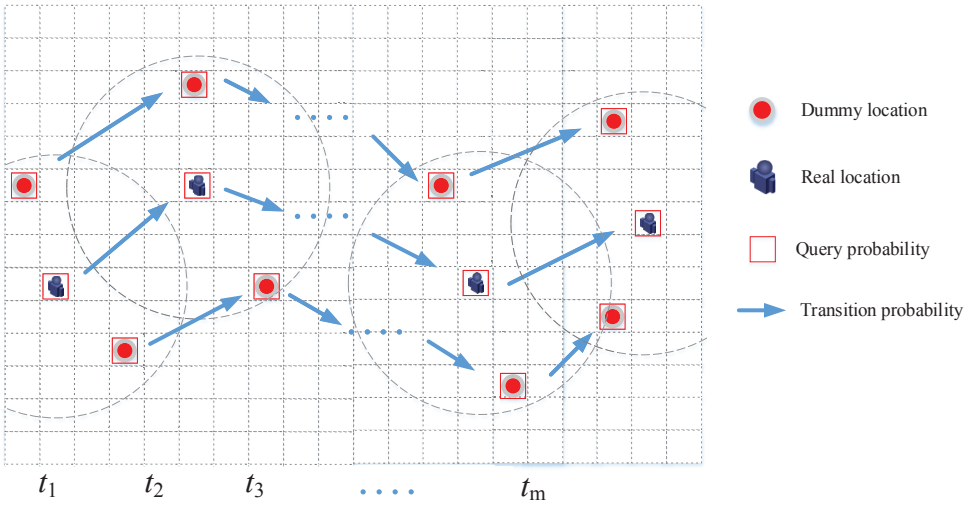

Figure 6. Dummy trajectories selection in trajectory publication.

4.3. Security Analysis

In this section, we analyze the security of our schemes. In the trajectory protection, the most vulnerable attacks are colluding attacks and inference attacks launched by the adversaries. We analyze the resistance of the schemes to the colluding attacks and the inference attacks as follows.

Resistance to Colluding Attacks. The colluding attack occurs when a group of users are connected to each other and share information. In other words, the adversary colludes with some other parties to deceive the rest parties to obtain the privacy information. Since both of the proposed schemes only runs on a separate module without including cooperation with other parties, so the proposed schemes can resist to colluding attacks.

Resistance to Inference Attacks. Inference attacks are launched by adversaries based on some pre-knowledge such as map information, query probability etc. Both of the proposed schemes generate dummies based on the gravity model. Since the gravity model is obtained by fitting the users' real historical data, it can accurately describe a user's real movement pattern. Therefore, the dummy trajectories generated are almost reasonable and meaningful trajectories, thus, it is difficult for the adversary to eliminate dummies by inference based on the information they have. As a result, the schemes can resist inference attack.

Conclusively, since our schemes use the gravity model and run on the separate module, they can resist to colluding attacks and inference attacks.

5. Experiments

In this section, we conduct simulation experiments to obtain the optimal coefficients of the gravity model and evaluate the privacy metric of the proposed trajectory protection schemes in continuous LBSs and trajectory publication by comparing them with the enhanced-DLS scheme, the optimal scheme and the random scheme. The optimal scheme does not consider the speed limit in generating the $k-1$ dummies with the maximum privacy metric. The random scheme considers the speed limit but randomly selects $k-1$ dummies. To evaluate their performances, we apply classical GPS-based Geolife datasets [45]. The trajectory dataset are composed of 17,621 trajectories of the pedestrians engaged in the Geolife test in Beijing within 50,176 hours. The total distance of the trajectories is 1,292,951 kilometers. These trajectories were recorded by different GPS loggers and GPS-phones. In our experiments, the sampling interval of the trajectory data is 1 minute. The maximum speed of users is 1.2 km/min. The simulation environment is Matlab R2014b. Specifically, simulation experiments include two parts:

- Obtaining the optimal coefficients of the gravity model to make the model fit the real users' datasets including commuting flows between two grids, the leaving flow for a grid, the arriving flow for a grid and the average distance between two grids.
- Evaluating the privacy metric of the proposed trajectory protection schemes in continuous LBSs and trajectory publication by comparing the proposed schemes with the enhanced-DLS scheme, the optimal scheme and the random scheme.

5.1. Optimal Coefficients

Figure 7a shows the trajectory of a user in a region. From Figure 7a, specifically, we can observe the moving direction, the location at every sampling moment and the grid that each location belongs to. In other wards, by analyzing Figure 7a, we can obtain the real-time data of users (i.e., such as the commuting flows, the leaving flow, the arriving flow and the average distance between two grids). Similarly, Figure 7b shows the trajectories of all the users within the region, and thus, the real data for all the users in the region including the commuting flows, the leaving flow, the arriving flow and the average distance between two grids can also be obtained through analyze Figure 7b. As a result, the optimal coefficients of the gravity model that meets all the real users' data can be calculated according Equation (15). The optimal coefficients are shown in Table 1.

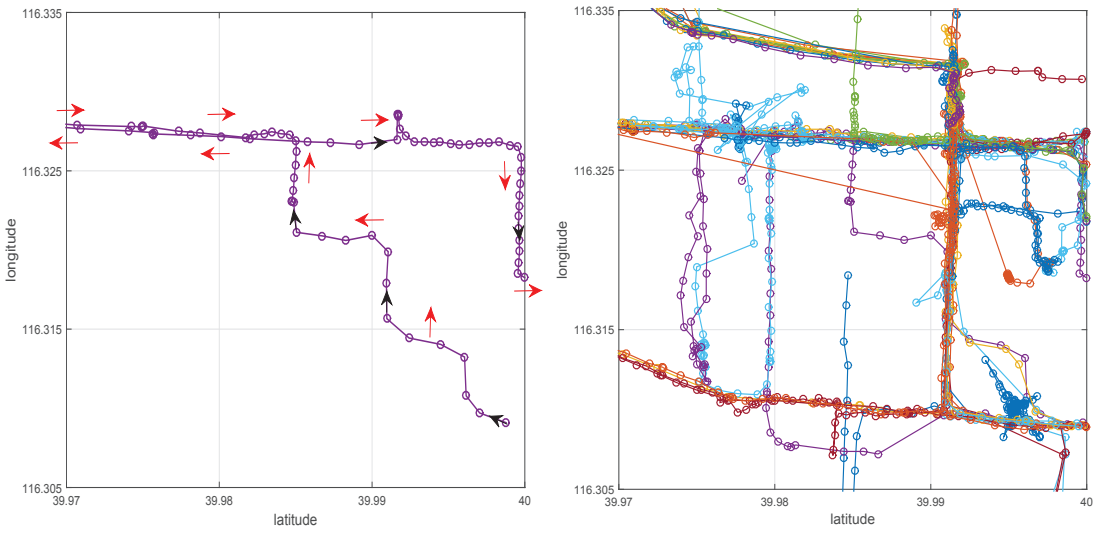

Figure 7. An illustration of user's trace and sample data of users' trace. (**a**) trajectory of a user; (**b**) trajectories of all users.

Table 1. The coefficients of gravity model.

Parameters	$\ln\alpha$	μ	θ	γ
Value	2.1813	1.303	1.0089	2.1

5.2. Evaluation of Privacy Performance

Figures 8–10 show the evaluations of privacy performance in terms of the running time and the entropy metrics including the continuous location entropy and trajectory entropy. The entropy metrics defined in Section 4.1 are used to quantify the uncertainty of the dummies generated by our schemes. When entropy metrics of a scheme is the high, the dummies generated by the scheme is uncertain. It means the adversaries are difficult to identify the users' real trajectory from the dummies, i.e., the privacy level of the scheme is high.

Figure 8 compares the continuous location entropy of the proposed trajectory protection scheme with the enhanced-DLS scheme, the optimal scheme and the random scheme. We can see that the continuous location entropies of the four schemes increase with the privacy factor k increasing. This is because the number of dummy trajectories increases with the increase of the privacy factor k. Therefore, it is more difficult to capture users' real-time locations. From Figure 8, it can be seen that the optimal scheme has the highest entropy for the same privacy factor k. This is because the optimal scheme selects dummy locations with the $k-1$ maximum entropies from the whole region to generate the $k-1$ dummy locations, while the other schemes select the dummy locations with $k-1$ maximum entropies within a reasonable limited region. Moreover, it can be seen that, for the same privacy factor k, the entropy of the proposed scheme is larger than those of the enhanced-DLS scheme and the random scheme. Compared with the enhanced-DLS scheme, the continuous location entropy of our scheme is improved by by 179.77%, 159.75%, 144.96%, 134.35%, 119.04% and 106.2%, when the privacy factors are 2, 3, 4, 5, 6 and 7, respectively. This means that the proposed scheme generates trajectories with better uncertainty, so it is very difficult for the adversaries to identity the real trajectory from the dummy trajectories, i.e., the privacy level of our scheme is high. This is because the enhanced-DLS scheme and the random scheme generate dummy locations without considering the user movement pattern, thus, resulting in great differences between the consecutive dummy locations which can be easily identified as dummy locations by adversaries.

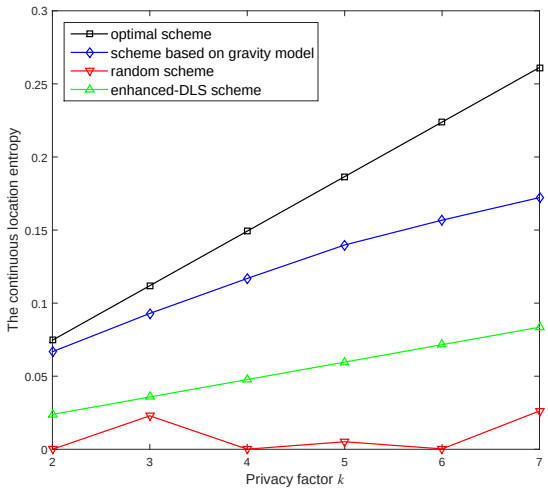

Figure 8. The continuous location entropy of different schemes.

Figure 9 compares the running time of the proposed scheme with the enhanced-DLS, the optimal scheme and the random scheme. It is seen that the running time of the four schemes increase with the increase of the privacy factor k. This is because the number of dummies increases with the increase of the privacy factor k, and thus, the schemes would spend more time to generate more dummies.

Moreover, It is seen that, for the same privacy factor k, the running time of the proposed scheme is larger than that of the random scheme and smaller than that of the optimal scheme. This is because the optimal scheme needs to traverse all the grids and calculate the $k-1$ maximum entropies of all grids to determine the dummies, while our scheme only needs to select the grids in a limited reasonable area and calculate the $k-1$ maximum entropies of the selected grids to determine the dummies. The random scheme directly selects k dummies randomly without comparing the entropy, hence, it spends less time than our scheme. In addition, we can see that when k is small, the enhanced-DLS scheme spends less time because the process of randomly allocating the transition probability requires less computing time.On the other hand, our scheme spends less time than the enhanced-DLS scheme when the k is large. This is because our scheme stores the transition probability, and enhanced-DLS schemes need to generate the transition probability randomly for each time.

Figure 10 compares the trajectory entropy of the proposed trajectory protection scheme with the optimal scheme and the random scheme. Similar to Figure 8, it can be seen that the trajectory entropies of the three schemes increase with the privacy factor k increasing. The trajectory entropy of the proposed scheme is larger than that of the random scheme and smaller than that of the optimal scheme. Moreover, the trajectory entropy performance of our scheme is 5.18 times higher than that of the random scheme on average. This means that the trajectories generated by our scheme have better uncertainty and are not easily cracked by the adversaries, i.e., the privacy level of our scheme is higher than that of other schemes.

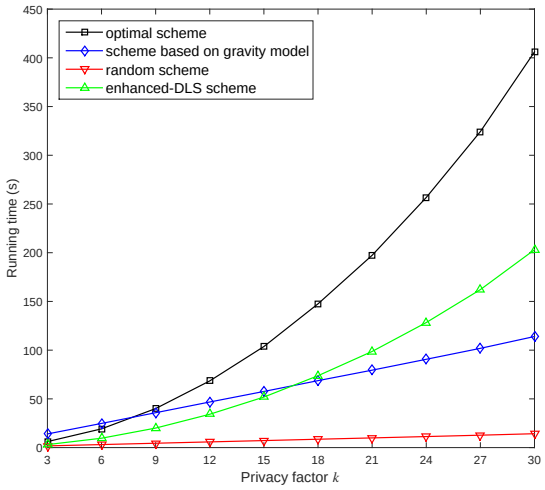

Figure 9. Running time of different schemes.

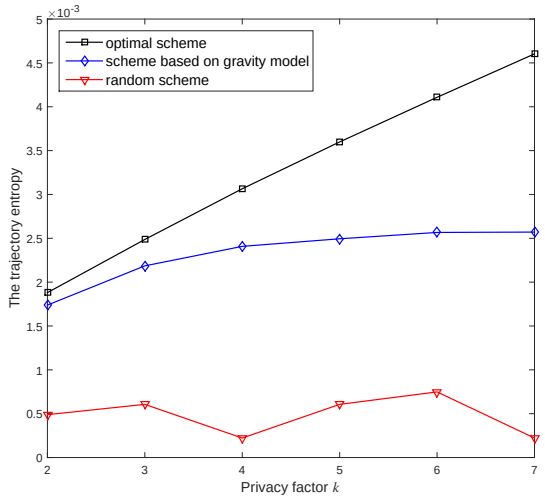

Figure 10. The trajectory entropy of different schemes.

6. Conclusions

In this paper, we proposed two trajectory protection schemes considering the movement pattern to protect the trajectory data in continuous LBSs and trajectory publication, respectively. Motivated by Jaynes' maximum entropy principle, in our paper, the continuous location entropy and the trajectory entropy based on the gravity are defined to measure the privacy level of the dummy trajectory. The schemes generate dummy trajectories according to entropy metrics. Simulations demonstrated that our schemes have better performances than the enhanced-DLS scheme and random scheme. Compared with the enhanced-DLS scheme, the continuous location entropy of our scheme is improved by 179.77%, 159.75%, 144.96%, 134.35%, 119.04% and 106.2%, when the privacy factors are 2, 3, 4, 5, 6 and 7, respectively. Moreover, the trajectory entropy of our scheme is 5.18 times higher than that of the random scheme. Since the entropy metric of our schemes is high, the dummies generated by the schemes are uncertain. It means the adversaries face difficulty in identifying the users' real trajectory from the dummies generated by our schemes, i.e., the privacy level of our schemes is high. In future work, we plan to study the trajectory protection in office buildings and residential communities based on the mobility models that describe user mobility pattern accurately in these areas.

Author Contributions: Conceptualization, Q.W. and C.Z.; Methodology, Q.W. and C.Z.; Software, C.Z. and H.L.; Writing—Original Draft Preparation, Q.W., C.Z. and H.L.; Writing—Review & Editing, Q.F., Z.L. and K.W.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 61701197, 61571108 and 61801379, the Project funded by China Postdoctoral Science Foundation under Grant No. 2018M641354, the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University, under Grant No. 2018D15 and the Natural Science Basic Research Plan in Shaanxi Province of China under Grant No. 2018JQ6057.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sun, G.; Chang, V.; Ramachandran, M.; Sun, Z.; Li, G.; Yu, H.; Liao, D. Efficient location privacy algorithm for Internet-of-Things (IoT) services and applications. *J. Netw. Comput. Appl.* **2017**, *89*, 3–13. [CrossRef]
2. La, H. A conceptual framework for trajectory-based medical analytics with IoT contexts. *J. Comput. Syst. Sci.* **2016**, *82*, 610–626. [CrossRef]
3. Lu, Y.; Xiong, K.; Liu, J.; Fan, P.; Zhong, Z. Optimal coordinated beamforming with artificial noise for secure SWIPT in multi-cell networks. *EURASIP J. Wirel. Commun. Netw.* **2018**, *2018*, 60. [CrossRef]
4. Lu, Y.; Xiong, K.; Fan, P.; Zhong, Z.; Letaief, K. Robust Transmit Beamforming With Artificial Redundant Signals for Secure SWIPT System Under Non-Linear EH Model. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2218–2232. [CrossRef]
5. Lu, Y.; Xiong, K.; Fan, P.; Zhong, Z.; Letaief, K. Coordinated Beamforming with Artificial Noise for Secure SWIPT under Non-Linear EH Model: Centralized and Distributed Designs. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1544–1563. [CrossRef]
6. Lu, Y.; Xiong, K.; Fan, P.; Ding, Z.; Zhong, Z.; Letaief, K. Global Energy Efficiency in Secure MISO SWIPT Systems with Non-Linear Power-Splitting EH Model. *IEEE J. Sel. Areas Commun.* **2008**, *10*. [CrossRef]
7. Xiong, K.; Chen, C.; Qu, G.; Fan, P.; Letaief, K. Group Cooperation with Optimal Resource Allocation in Wireless Powered Communication Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3840–3853. [CrossRef]
8. Xiong, K.; Wang, B.; Liu, R. Rate-Energy Region of SWIPT for MIMO Broadcasting under Nonlinear Energy Harvesting Model. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5147–5161. [CrossRef]
9. Gao, S.; Ma, J.; Sun, C.; Li, X. Balancing trajectory privacy and data utility using a personalized anonymization model. *J. Netw. Comput. Appl.* **2013**, *38*, 125–134. [CrossRef]
10. Fechner, T.; Kray, C. Attacking location privacy: Exploring human strategies. *ACM Conf. Ubiquitous Comput.* **2012**, 95–98. [CrossRef]
11. Ye, M.; Yin, P.; Lee, W.; Lee, D. Exploiting geographical influence for collaborative point-of-interest recommendation. In Proceedings of the 34th International ACM SIGIR Conference on Research and Development in Information Retrieval, Beijing, China, 24–28 July 2011; pp. 325–334. [CrossRef]

12. Wang, H.; Li, Q.; Yi, F.; Li, Z.; Sun, L. Influential spatial facility prediction over large scale cyber-physical vehicles in smart city. *EURASIP J. Wirel. Commun. Netw.* **2016**, *2016*, 103. [CrossRef]
13. Ivanov, R. Real-time GPS track simplification algorithm for outdoor navigation of visually impaired. *J. Netw. Comput. Appl.* **2012**, *35*, 1559–1567. [CrossRef]
14. Kido, H.; Yanagisawa, Y.; Satot, T. An anonymous communication technique using dummies for location-based services. In Proceedings of the International Conference on Pervasive Services, Santorini, Greece, 11–14 July 2005; pp. 88–97. [CrossRef]
15. Bindschaedler, V.; Shokri, R. Synthesizing plausible privacy-preserving location traces. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016.
16. Lei, P.; Peng, W.; Su I.; Chang, C. Dummy-based schemes for protecting movement trajectories. *J. Inf. Sci. Eng.* **2012**, *28*, 335–350.
17. Xu, T.; Cai, Y. Exploring historical location data for anonymity preservation in location-based services. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008. [CrossRef]
18. Xu, T.; Cai, Y. Feeling-based location privacy protection for location-based services. In Proceedings of the 16th ACM conference on Computer and communications security, Chicago, IL, USA, 9–13 November 2009; pp. 348–357. [CrossRef]
19. Wu, X.; Sun, G. A novel dummy-based mechanism to protect privacy-aware location-based services. In Proceedings of the 2014 IEEE International Conference on Data Mining Workshop, Shenzhen, China, 14 December 2014. [CrossRef]
20. Niu, B.; Gao, S.; Li, F.; Li, H. Protection of location privacy in continuous LBSs against adversaries with background information. In Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, USA, 15–18 February 2016; pp. 1–6. [CrossRef]
21. Kini, A.; Kulkarni, S. Real Time Implementation of k fake Location Generation Algorithm to Protect Location Privacy in Location Based Services. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 13–16 September 2017. [CrossRef]
22. Peng, T.; Liu, Q.; Wang, G. Enhanced Location Privacy Preserving Scheme in Location-Based Services. *IEEE Syst. J.* **2017**, *1*, 219–230. [CrossRef]
23. Terrovitis, M.; Mamoulis, N. Privacy Preservation in the Publication of Trajectories. In Proceedings of the Ninth International Conference on Mobile Data Management, Beijing, China, 27–30 April 2008. [CrossRef]
24. Chen, R.; Fung, B.; Desai, B. Differentially Private Trajectory Data Publication. *arXiv* **2011**, arXiv:1112.2020.
25. Abul, O.; Bonchi, F.; Nanni, M. Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases. In Proceedings of the IEEE 24th International Conference on Data Engineering, Cancun, Mexico, 7–12 April 2008. [CrossRef]
26. Pensa, R.; Monreale, A.; Pinelli, F.; Pedreschi, D. Pattern-Preserving k-Anonymization of Sequences and its Application to Mobility Data Mining. In Proceedings of the PiLBA '08 Privacy in Location-Based Applications, Malaga, Spain, 9 October 2008, pp. 44–60.
27. Nergiz, M.; Atzori, M.; Saygin, Y. Towards Trajectory Anonymization: A Generalization-Based Approach. In Proceedings of the SPRINGL '08 Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, Irvine, CA, USA, 4 November 2008; pp. 52–61. [CrossRef]
28. Niu, B.; Li, Q.; Zhu, X.; Cao, G.; Li, H. Achieving k-anonymity in privacy-aware location-based services. In Proceedings of the IEEE INFCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 754–762. [CrossRef]
29. Erlander, S.; Stewart, N.F. *The Gravity Model in Transportation Analysis*; VSP: Utrecht, The Netherlands, 1990.
30. De Dios Ortuzar, J.; Willumsen, L.G. *Modelling Transport*; John Wiley and Sons: Chichester, UK, 2001.
31. Davies, W.K. Urban connectivity in montana. *Ann. Reg. Sci.* **1979**, *13*, 29–46. [CrossRef]
32. Jung, W.S.; Wang, F.; Stanley, H.E. Gravity model in the Korean highway. *EPL-Europhys. Lett.* **2008**, *81*, 48005. [CrossRef]
33. Krings, G.; Calabrese, F.; Ratti, C.; Blondel, V. Urban Gravity: A Model for Intercity Telecommunication Flows. *J. Stat. Mech. Theory Exp.* **2009**, *2009*. [CrossRef]
34. Tomita, S.; Hayashi, Y. Spatial analysis of centralization and decentralization in the population migration network. In Proceedings of the Asia-Pacific Symposium on Information Visualisation, APVIS 2006, Tokyo, Japan, 1–3 February 2006; pp. 41–47.

35. Zhang, J.; Chow, C. Spatiotemporal sequential influence modeling for location recommendations: A gravity-based approach. *Trans. Intell. Syst. Technol.* **2015**, *7*, 1–25. [CrossRef]
36. Wang, Y.; Yuan, N.; Lian, D.; Xu, L.; Xie, X.; Chen, E.; Rui, Y. Regularity and Conformity: Location Prediction Using Heterogeneous Mobility Data. In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Sydney, NSW, Australia, 10–13 August 2015; pp. 1275–1284. [CrossRef]
37. Xiong, K.; Fan, P.; Lu, Y.; Letaief, K.B. Energy efficiency with proportional rate fairness in multirelay OFDM networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 1431–1447. [CrossRef]
38. Wang, Q.; Wu, D.; Fan, P. Delay-constrained optimal link scheduling in wireless sensor networks. *IEEE Trans. Veh. Technol.* **2010**, *59*, 4564–4577. [CrossRef]
39. Zhang, C.; Fan, P.; Xiong, K.; Fan, P. Optimal power allocation with delay constraint for signal transmission from a moving train to base stations in high-speed railway scenarios. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5775–5788. [CrossRef]
40. Kang, J.; Fan, P.; Cao, Z. Flexible construction of irregular partitioned permutation LDPC codes with low, error floors. *IEEE Commun. Lett.* **2005**, *9*, 534–536. [CrossRef]
41. Jaynes, E.T. Information Theory and Statistical Mechanics II. *Phys. Rev.* **1957**, *108*, 171–190. [CrossRef]
42. Parra-Arnau, J.; Rebollo-Monedero, D.; Forné, J. Measuring the privacy of user profiles in personalized information systems. *Futur. Gen. Comput. Syst.* **2014**, *33*, 53–63. [CrossRef]
43. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley-Blackwell Publication: Hoboken, NJ, USA, 2006; ISBN 9780471241959.
44. Trevor, H; Robert, T.; Jerome, F. *The Elements of Statistical Learning*, 2nd ed.; Springer-Verlag: New York, NY, USA, 2009; ISBN 978-0-387-84858-7.
45. Zheng, Y.; Xie, X.; Ma, W. GeoLife: A Collaborative Social Networking Service among User, Location and Trajectory. *IEEE Data Eng. Bull.* **2010**, *33*, 32–40.