Grid Anonymous Trajectory Privacy Protection Algorithm Based on Differential Privacy

Hong Dai*, Zijian Wu, Shuang Wang, and Ke Wu

***Abstract*— Attackers can use data analysis to learn about the user's regular habits if the current trajectory data is shared and used without being processed. It will lead to the user's private information being revealed. To meet the trajectory k-anonymity, the method of anonymity protection that considers the entire trajectory as a unit frequently needs ample anonymity space and noise addition. Research has focused on finding practical and effective ways to protect trajectory data. As a result, the article suggests the Differential Privacy for Grid Anonymous Trace Privacy (DP-GATP) method. First, Term Frequency and Inverse Document Frequency (TF-IDF) technology extracts the crucial dwell point data from the user trajectory. Different weights are then assigned based on the authorization level for privacy protection. The exponential technique is used to reduce noise and fairly distribute the privacy budget. The geographical grid then changes the trajectory data coordinates. For *k*-clustering, the grid weight greedy clustering technique is employed. The experimental findings demonstrate that the strategy may safeguard the privacy of critical dwell spots in trajectory data under the assumption of assuring data availability. The amount of anonymous space needed to publish data significantly decreases after grid processing. When compared to algorithms of a similar nature, the availability of the data published is higher.**

***Index Terms*— *K*-Anonymity Trajectory, Grid Anonymous Trace Privacy, Privacy Protection Algorithm, Index Mechanism, Laplace Noise**

I. Introduction

With the continuous development of new-generation information services such as mobile positioning, some location-based services have penetrated into people's daily life [1]. So far, location-based services involve many areas of people's life, including navigation, express delivery, and rescue. The continuous development of China's 5G technology has promoted communication speed. But there are also security risks of information leakage. Data privacy protection has become a hot topic of current research.

Manuscript received January 15, 2023; revised July 5, 2023. This work is supported by Graduate Education Reform and Innovation Project, University of Science and Technology Liaoning (LKDYC202221)

Hong Dai is a Professor of the School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, CO 114051, China (corresponding author: tel:+086-18642268599; fax: 0412-5929818;e-mail: dear_red9@163.com).

Zijian Wu is Postgraduate of the School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, CO 114051, China (e-mail: 939674778@qq.com).

Shuang Wang is Postgraduate of the School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, CO 114051, China (e-mail: Wangshuang9712@163.com).

Ke Wu is Postgraduate of the School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan, CO 114051, China (e-mail: 786854814@qq.com).

The location-based services will also be applied to broader fields, and they have strong commercial value [2]. However, when the trajectory data is not processed, it will let out a large amount of user-sensitive information, such as the user's family address and workplace. The attacker can obtain the living habits and behavior rules of users by analyzing a large amount of trajectory data. The track data contains a large amount of personal information, such as personal privacy data, personal health status, and behavioral habits. Due to the exposure of sensitive personal information, the release of unencrypted track data will have a detrimental effect on people. Montjoye [3] looked at how much the user spent on credit cards in a European nation. According to the four users' credit card consumption data, it was determined that more than 85% of the users could be identified merely by the time information and location information. The user's private information may, at any moment, be made public. In recent years, certain makers of mobile phone brands also released the "privacy tracking door" incident [4]. Without the users' knowledge, mobile phone manufacturers can regularly upload users' accurate location information to the company via the built-in application software. There are numerous examples of this. It is critical to process the trajectory data to protect personal privacy. An effective data privacy and security protection mechanism has gotten a lot of attention both at home and abroad [5-6].

At present, trajectory privacy protection algorithms are mainly divided into four categories [7]: trajectory suppression technology, trajectory k-anonymity, changing pseudonyms, and false trajectory. The earliest differential privacy trajectory data research was based on Chen Rui [8] and others. The research teams proposed the prefix tree publishing trajectory dataset method Société de transport de Montréal (STM). The technique can protect privacy parameters by constructing the prefix tree reconstruction dataset. However, the availability of data will decline after publishing.

A variable-length *n*-grams model was put forth by Xiaoli Xiong et al. [9]. The model extracted the trajectory data structure based on variable length. It can have a good performance in feature extraction. Jiang et al. [10] judged the possible direction and distance of the next position point by analyzing the maximum speed of the track and adding noise. Tian Feng et al. [11] divided the entire map into multiple grids and numbered them using the Hilbert curve. They created a track prefix tree and allocated a reasonable privacy budget to each grid by analyzing the relationship between adjacent grids. Hua Jinyu et al. [12]

calculated the distance between trajectories and combined the nearest positions the next time. They finally added noise to the corresponding generalization area to publish the trajectory dataset with the same length as the original trajectory. Li Meng et al. [13] used the k-means method to cluster the same time position in the trajectory dataset. They added noise to each cluster member according to the clustering results. The improved method can effectively prevent excessive noise based on the Laplace.

This paper proposes DP-GATP, the differential privacy for grid anonymous trace privacy algorithm based on the current state of data privacy research at home and abroad, in response to several hot issues such as large coverage area and difficulty of dwell point extraction protection in trajectory data. Firstly, the dwell points are scored by the TF-IDF text weighting technique, and the trajectory data are extracted and classified into three categories of dwell points according to their importance according to the scoring results. To allocate the privacy budget reasonably, the exponential mechanism and Laplace noise are used to perturb the noise of the dwell points and combine with the idea of infinite series. Then, the algorithm is applied to the T-Driver dataset. The trajectory data are converted from spatial to temporal coordinates following grid processing. Finally, the grid weight clustering algorithm is used to *k*-anonymize the grid trajectories, resulting in the anonymization of the published data. When compared to similar algorithms, the DP-GATP algorithm provides more data availability.

II. METHODOLOGY

Dwork et al. [14] proposed the differential privacy model in 2006. The model makes it impossible to identify whether or not a record exists in the original data table by randomly disturbing the published data regardless of the attacker's background knowledge. The advantage of the model is that it does not need special attack assumptions. At the same time, it does not care about the background knowledge of the attacker. Lastly, a lot of analysis is given to represent the risk of privacy disclosure. The concept of the adjacent dataset is first introduced in order to introduce differential privacy. It is described in definition.

Definition 2.1: The symmetrical difference is recorded as $|D \Delta D'|$ between the datasets D and D'. The datasets D and D' have the same attribute structure. They are called the adjacent datasets if $|D \Delta D'|=1$.

Definition 2.2: Algorithm *K* is said to provide ε-differential privacy [15] protection if differential privacy satisfies formula 1.

$$\Pr[K(T_1) \in S] \le \exp(\varepsilon) \times \Pr[K(T_2) \in S] \quad (1)$$

Pr[.] represents the probability of the event. Parameter ε is the privacy protection budget. The parameter determines the privacy protection degree of the algorithm. The smaller ε is, the higher the privacy protection degree is. The larger ε is, the lower the privacy protection degree is.

Definition 2.3: The differential privacy achieved by adding random noise to the numerical query results is called the Laplace mechanism. The random noise obeys Laplace distribution. Laplace distribution is known as a double exponential distribution. The probability density is shown in Fig.1. Its probabilistic density function is given as follows (formula 2):

$$\Pr(x) = \frac{1}{2\lambda} e^{-\frac{|x-\mu|}{\lambda}} \quad (2)$$

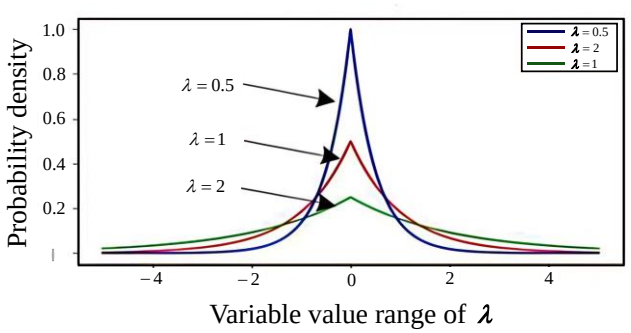

Fig.1. The Laplace probabilistic density function diagram

λ is the scale parameter, and μ is the position parameter. The position parameter μ is usually set to zero during the adding noise process to make the adding noise data closer to the original data.

Definition 2.4: For non-numeric queries, differential privacy uses the exponential mechanism to randomize the results. The output result is *Ran*(*A*) if the dataset *D* and the random algorithm *A* are given. ***r*** is an entity object in *Ran*(*A*). It satisfies condition $r \in Ran(A)$. $g(D,r) \to R$ is the scoring function of *R*. Δg is the sensitivity of $g(D,r)$. We can know that algorithm *A* provides ε-differential privacy protection if the algorithm helps formula 3:

$$A(D,g) = \left\{ r: \left| \Pr[r \in Ran(A)] \infty \exp\left(\frac{\varepsilon g(D,r)}{2\Delta g} \right) \right. \right\} \quad (3)$$

Two important combinatorial properties of differential privacy are described below. Sequence combination properties are described below.

$M_1, M_2, ..., M_n$ are the different algorithms. The combined sequence of the algorithm $\{M_1, M_2, ..., M_n\}$ provides $\sum_{i=1}^{n} \varepsilon_i$-differential privacy protection for the same dataset *D* if ε_i-differential privacy is satisfied respectively.

Parallel combination properties are described below. Let algorithms M_i satisfy ***s***-difference privacy $1 \le i \le n$. The parallel combination of algorithms provides max ε_i-differential privacy for different datasets $\{D_1, D_2, ...D_n\}$. The property shows that the privacy protection level is the lowest of all algorithms when the differential privacy protection algorithm is applied to multiple disjoint datasets, that is, the largest privacy budget.

Definition 2.5: TF-IDF is shortened form of the term frequency-inverse document frequency. It is a weighting technique based on statistical methods. TF-IDF is commonly used in search engines and text mining. Word frequency refers to the number of words in a document as a percentage of the total number of words in the document. It reflects the importance of the word to the document from the side. The smaller the probability of anti-text is, the greater the difference between the document and the word. Assume the tracking dataset is regarded as a document set. Each track is a document, and each dwell point is a word in the document. The dwell point is very important to the user

if a dwell point frequently appears in a track and rarely appears in the whole track dataset or a dwell point frequently appears in a track and the whole track dataset. Assume the trajectory dataset is D and the trajectory is expressed as W_d, TF-IDF value $W_f(S_i)$ of any dwell point S_i can be shown as follows (formula 4):

$$W_f(S_i) = \frac{R_d(S)}{\sum_{S_j \in T_d} R_d(S)} \times \log\left(\frac{|D|}{|\{R_d | R_d(S) \geq S_t, R_d \in D\}|}\right) \quad (4)$$

$R_d(S_i)$ represents the dwell time of dwell point S_i. S_t is the time threshold determined as the dwell point. $|D|$ is the total number of tracks contained in the track dataset.

III. Experiments

The trajectory data includes the user's daily travel route and much important sensitive location information such as home address and workplace. Some geographic locations carry rich semantic information, for example, hotels and hospitals. The user's trajectory often contains multiple dwell points. Different dwell points mean different geographic location information and semantic information. The existing track information is shown in Fig.2. Home and workplace belong to the important dwell point information. It contains important semantic information. It often reflects users' living habits. Location information, such as service stations and gas stations, contains less privacy information, and the information is less important.

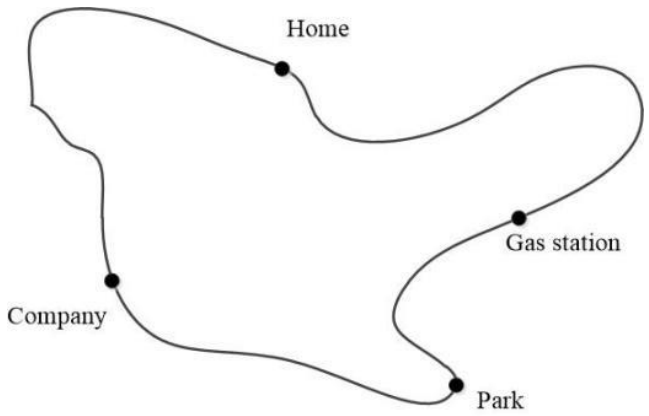

Fig.2. Schematic diagram of trajectory stop point semantic information

The longitude and latitude coordinates of track data can reflect the location address of the current user. The movement threshold T_s of the dwell point is set to 40km. $\left(X_{T_i}, Y_{T_i}\right)$ is the track positional coordinate of the dwell point at a certain time. The time threshold of the dwell point is set to 1200 seconds. It is regarded as an unreasonable movement if the speed of the GPS signal exceeds 120km/h because the track data is the signal collected by GPS. One thousand two hundred seconds is the uniform value of the collected signal. The upper limit of trajectory movement is 40km in 1200 seconds. The disturbance radius is set to 5km. T_{Mi} is the timestamp of the track at the moment, M_i. The position information will be extracted as the dwell point if one of the two conditions of formulas (5) and formulas (6) or formulas (6) and formulas (7) is satisfied. Meanwhile, the trajectory data stops at a certain position or moves slowly.

$$S_{T_1T_2} = \sqrt{\left(X_{T_2} - X_{T_2}\right)^2 + \left(Y_{T_2} + Y_{T_1}\right)^2} \quad (5)$$

$$S_{T_1T_2} < T_S \quad (6)$$

$$T_{M_i} - T_{M_{i-1}} > 1200 \quad (7)$$

The following dwell point scores are obtained according to the statistical results of TF-IDF technology. The selected dwell points are divided into three classes according to their importance. The three classes are important, general, and low. At the same time, it also serves as the basis for adding privacy protection and adding privacy budget for different dwell points. The final score is shown in Table I after extraction of the dwell point.

TABLE I

THE DWELL POINT SCORES

Text frequency	Dwell point	Classification criteria
High	Hospital, Home, Company	Class I
High	Parks, Hotels	Class II
Low	Service station, Gas station	Class III

The rest of the noise disturbance points will be filtered out from the dwell point in the trajectory data within the disturbance radius after the privacy budget is allocated. The data point will have the original noise disturbance point **A** after exponential disturbance. It will be converted into noise disturbance point B according to the random disturbance result. According to the response privacy budget allocation sequence, the corresponding Laplace noise will be added. Fig.3 depicts the residence point disturbance process.

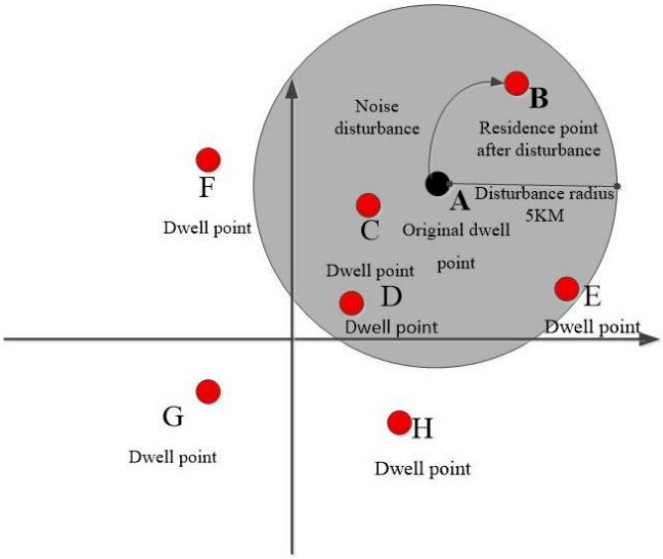

Fig.3. Dwell-point disturbance process

After all dwell point data is disturbed, the original dataset is replaced with the noise dataset. The noise dataset not only conforms to the definition of differential privacy but also retains statistical significance. The noise dataset will not cause privacy disclosure to the real users contained in the dataset. Table II displays the budget allocation and noise disturbance procedure method.

TABLE II
BUDGET ALLOCATION AND NOISE DISTURBANCE PROCESS ALGORITHM

Input: Track dataset fragment H={$Spart_1$,...,$Spart_n$}, Privacy budget ε
Output: Trajectory segments satisfying differential privacy *D*

```
for i=1 to n do
  calculate Sp_list_i      // Use formula 4 to calculate Sp_list_i
  store Sp_list_i          // store Sp_list_i in the set
 for j=1 to n do
  Sp_list_ij ← Sp_list_i
  Laplace(Sp_list_ij)      //Add Laplace noise to each Sp_list_ij
 end for
end for
return D
```

$|D|$ is the length of each track data segment. The time complexity of the algorithm is $O(*|D|)$ according to the analysis of the minimum execution times of the algorithm. The trajectory data is represented as TR= {< x_1, y_1, t_1>,< x_2, y_2, t_2>, ⋯, < x_n, y_n, t_n>} in space-time coordinates. The space-time information has a long spatial coverage. The track TR is converted into the grid sequence TPR if the space-time coordinates have meshed.

TPR={< tb_1, te_1, $grid_1$>,< tb_2, te_2, $grid_2$>,⋯,< tb_n, te_n, $grid_n$>}. $grid_i$ is the grid number of track segment *i*, and the track segment numbers from left to right are {1,2, ..., *n*}. The spatial meshing process is shown in Fig.4.

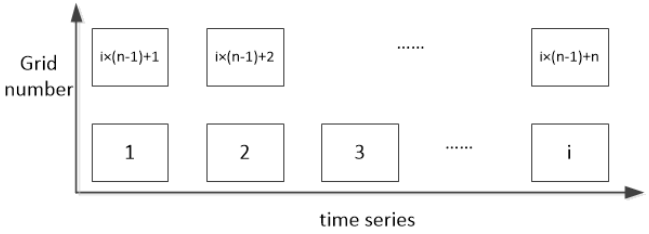

Fig.4. Spatial grid division

The grid is divided according to time, and each grid represents different periods. The space-time coordinates *tr* of trajectory data will fall into different grid sequences according to different timestamps. The grid number will increase from left to right according to the division of the grid sequence. Different grid parameters are set to different values of grid sequence.

The walking area of the track is marked in the spatial grid division of the track to make the track data in the grid *k*-anonymous. The trajectory distance from the first grid to the 80*th* grid is three under the grid distance division. The grid sequence and one of the tracks are described in Fig.5.

The trajectory data points are scattered and stored in each grid after the trajectory data is converted from *tr* to grid sequence *TPR*. Firstly, the grid weight greedy clustering algorithm is used to anonymize the trajectory data of the data points in the grid. The flow of the algorithm is as follows.

Step 1: Set the current suction factor *sfactor*=1 and initialize the 78×78 grid sequence. Then store track data points.

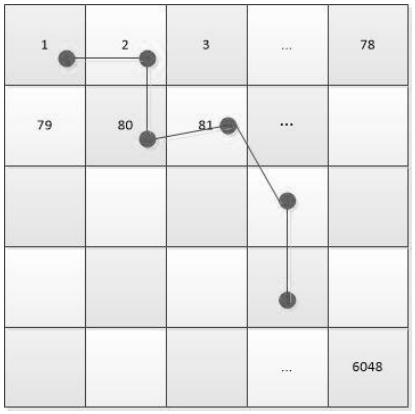

Fig.5. Track grid sequence under the grid division

Step 2: Count the number of track points of each grid and initialize the optimal value weight parameter *Max_weight* =0. The more track grid points are, the higher the weight index of the grid is. *Max_weight* is set to the value of *current_weight* if the current weight index is *current_ weight* > *Max_weight*.

Step 3: Set the grid of the *Max_weight* point as the cluster center after the search is completed. Select *k*-1 track segments whose distance from the current cluster center is less than the suction factor *sfactor*. The *k* track segments at this time are removed from the dataset, and the operation is repeated after reaching *k* values.

Step 4: Save the current factor value *sfactor* if the clustering is successful. Try to reduce the value *sfactor* and call the procedure of Step 3 again. It indicates that the current suction factor is too small to achieve the effect of *k*-anonymous if clustering fails. Therefore, the suction factor will be increased, and Step 3 will be repeated. Finally, it quickly converges to the most appropriate distance threshold. The suction factor saves the value of the current suction factor *sfactor*. Ensures that the currently obtained dataset *k*-anonymous is the most reasonable anonymous set solution.

The experimental dataset is the network public dataset *t*-driver widely used in the research of trajectory data publication. More than 10,000 taxis from Beijing in 2008 are included in the dataset. The dataset covers more than 15 million track coordinate points. Based on the fact that Beijing spans more than 9 million kilometers, the track's total distance coverage area is calculated. Each rental car in the dataset has a different set of track points, with a track collection number ranging from 600 to 20000. The dataset includes important dataset fields such as vehicle ID, time axis, longitude, and dimension. The sampling frequency of GPS ranges from 1 second to 10 minutes. The data fields are shown in Table III. The configuration environment of the experiment is shown in Table III.

TABLE III
THE T-DRIVER DATASET

field	semantic information
Vehicle ID	Identification ID of taxi vehicle
Timestamp date	Year, month and day information of timestamp
longitude	Position longitude of vehicle current timestamp
dimension	Location dimension of vehicle's current timestamp

The experiment extracted 1000 cab trajectory data as the

experimental environment configuration test data. The data are divided into five groups, containing more than 600,000 trajectory points. The first two groups of data are used for TF-IDF dwell point labeling and grid partitioning experiments, and the last three groups of data are used for DP-GATP algorithm experiments and comparison test verification. The original trajectory data distribution map of the trajectory can not only visually reflect the area covered by the trajectory but also analyze the hidden dwell point location information. The experimental data were reproduced by Matlab simulation to show the original data trajectory distribution of the five groups of trajectory data in the dataset. From the analysis of data plotting, a large number of trajectories of cabs cover the area within the fourth ring of Beijing, and the area covered is relatively dense and uniform. Due to the deterministic coordinates of the trajectories, it is convenient to extract the stopping point location information from the trajectories.

This experiment uses the root mean square error to test the effectiveness of the algorithm, and the RMSE value is expressed as follows (formula 8):

$$RMSE = \sqrt{\frac{\sum_{t=1}^{L} \left\| \mathrm{P}_t - r_t \right\|_2}{L}} \tag{8}$$

RMSE can measure the deviation degree between the original trajectory and the published trajectory. The smaller the deviation, the closer the release trajectory is to the original trajectory after differential privacy protection. Where p_t denotes the location point of the original trajectory, r_t denotes the published trajectory, and L represents the length of the trajectory data. The optimal grid division sequence is obtained as a 78×78 grid according to the grid optimum solved above, which covers a total of one week of timestamps according to the timestamp distribution of the T-Driver dataset, and thus the overall number of seconds of timestamps is found to be 604,800 seconds. The grid is made up of 78 horizontal cells and 78 vertical cells. Each grid has a time coverage edge of 100 seconds.

The paper proposes the DP-GATP algorithm in different privacy budgets ε. A total of 7 semantic dwell points for the three types are compared and analyzed on the T-Driver dataset in the paper. The general value is within 1. It means that the algorithm provides differential privacy protection. Therefore, the values of experimental parameters are set to 0.2, 0.4, 0.6, 0.8, and 1. The experimental results are shown in Fig.6.

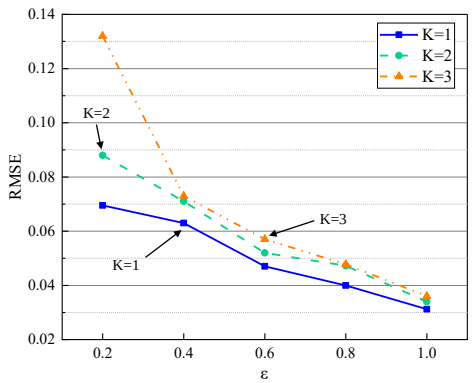

Fig.6. Availability comparison of the first type

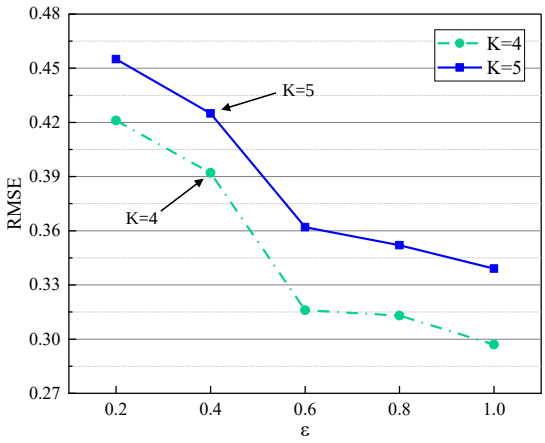

Fig.7. Availability comparison of the first type and the second type

It can be concluded that the privacy budget is directly proportional to the data available from the below experimental results. When the added privacy budget is larger, it means that the smaller the degree of data protection is, the stronger the data available is. When the added privacy budget is smaller, it means that the greater the degree of data protection is, the weaker the availability of data is.

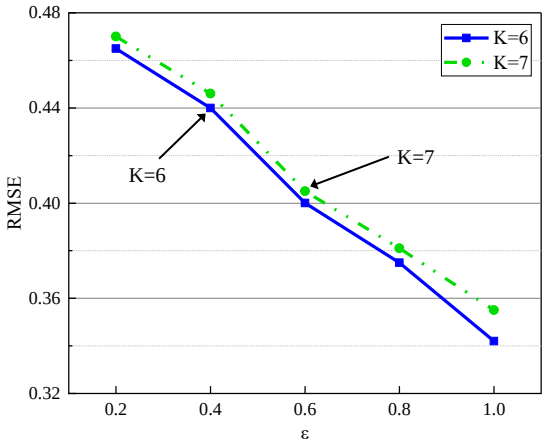

Fig.8. Availability comparison from the first type to the third type

The DP-GATP, the GIDP [15], and the Laplace noise algorithm are compared in the experiment. Laplace noise algorithm is the most basic data disturbance function [16]. The disturbance has certain randomness and uncertainty because the fluctuation range of the disturbance has not been fully explored theoretically. The disturbing noise is used as an original disturbance indicator for experimental reference. The GIDP algorithm has high academic value as a classical algorithm in the field of differential privacy trajectory data publication. The GIDP algorithm proposes a privacy protection framework in location-based applications. The algorithm fully considers the required protection level and the background knowledge of attackers. The algorithm also defines the intuitive concept of protecting the user's position within the radius *r* through the indistinguishable geographical mechanism. The noise protection stability of the algorithm is enhanced by adding random noise. It is combined with the geographical indistinguishable mechanism. Therefore, the GIDP algorithm has a good comparative effect. The DP-GATP

algorithm, the GIDP algorithm, and the Laplace algorithm are used to verify the first type of dwell point according to the importance of the dwell point in Fig.9. Then, the three algorithms are also used to verify the first type and the second type of dwell point in Fig.10. At last, the three algorithms are used to verify from the first type to the third type again in Fig.11. Therefore, the experimental results further confirm that the privacy budget is directly proportional to the data availability in Fig.9, Fig.10, and Fig.11.

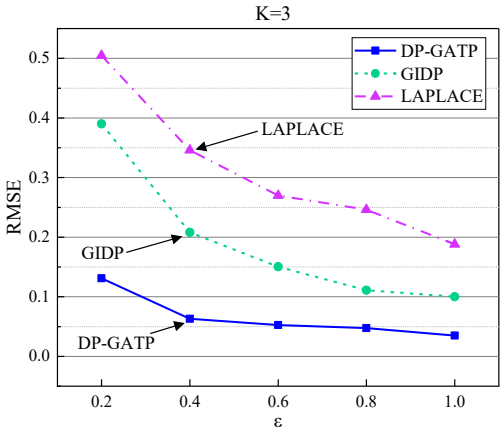

Fig.9. Comparison of different algorithms in the first type

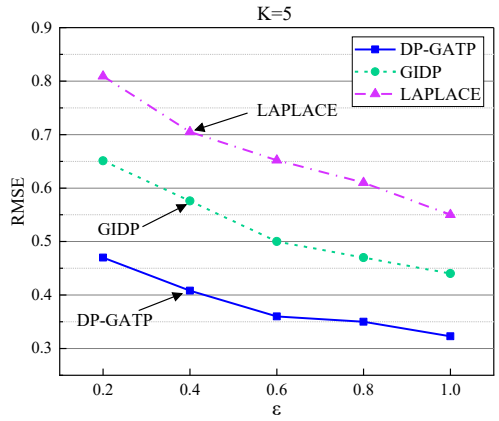

Fig.10. Comparison of different algorithms for the first type and the second type

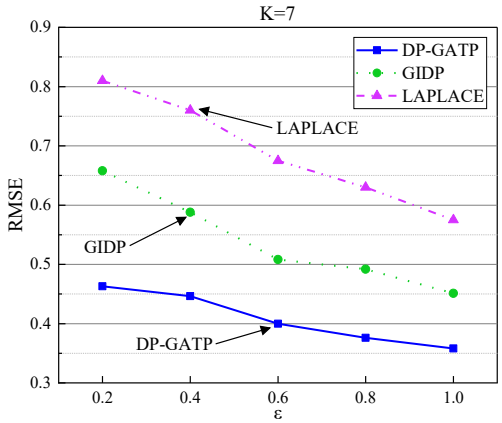

Fig.11. Comparison of different algorithms from the first type to the third type

IV. Conclusion

The paper proposes a grid anonymization differential privacy protection algorithm DP-GATP to aim at the research problem of differential privacy trajectory publishing. Firstly, the algorithm uses TF-IDF to select and score important dwell points. It not only filters out the dwell points containing important semantic information but also searches for disturbance candidate points within the disturbance radius according to the election results of dwell points. They are divided into three levels according to the scoring results and the importance of dwell points. The privacy sequence is assigned to each dwell point according to the grade scoring results and the idea of infinite series. After the spatial transformation of the space-time grid, the size of the suction factor is adjusted through the grid weight clustering algorithm to find the optimal suction factor. The optimal suction factor achieves the effect of optimal publishing of the *k*-anonymous trajectory dataset. Meanwhile, it solves the difficult problem of protecting key privacy information in trajectory data publishing.

The algorithm proposed in this paper is still a worthwhile research topic in terms of temporal trajectory datasets as well as grid partitioning. Future work can consider how to publish trajectory datasets in an effective interactive platform. The platform needs decentralized and maximum background knowledge of the attacker factor and so on. The platform enables the interactive operation of published datasets between the platform and the user. In the future, we can consider how to add more effective noise disturbance and divide the anonymous track interval with finer granularity under grid processing. Additionally, it's a useful technology to grow. Future research on the intersection of privacy protection and block chain technology will likewise gain popularity.

References

[1] Youhua Xia, Libing Wu, Zheng Xi, Tianqi Tian, and Jiong Jin, "Data Dissemination With Trajectory Privacy Protection for 6G-Oriented Vehicular Networks," IEEE Internet of Things Journal, vol.9, no.21, pp21469-21480,2022.

[2] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila, "A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects," IEEE Communications Surveys and Tutorials, vol.23,no.2, pp1160-1192, 2021.

[3] Yves-Alexandre de Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel, "Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports, vol.3, no.1, pp1-5, 2013.

[4] Qiang Gao, Fengli Zhang, Ruijin Wang, and fan Zhou, "Trajectory big data: a review of research on key technologies in data processing," Journal of software, vol.28, no.04, pp959-992, 2017.

[5] Tianqing Zhu, Gang Li, Wanlei Zhou, and Philip S. Yu, "Differentially private data publishing and analysis: A survey," IEEE Transactions on Knowledge and Data Engineering, vol.29, no.8, pp1619-1638, 2017.

[6] M. Kangwa, C.S. Lubobya, and J. Phiri, "Protection of personally identifiable Information and Privacy via the use of Hardware and Software," Lecture Notes in Engineering and Computer Science, vol.2243, pp75-81, 2021.

[7] Zhaowei Hu, and Jing Yang. "Analysis on research progress of trajectory privacy protection technology," Computer Science, vol.43, no.04, pp16-23, 2016.

[8] Rui Chen, Benjamin C. M. Fung, Bipin C. Desai, and Nériah M. Sossou, "Differentially private transit data publication: A case study on the montreal transportation system," Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 12-16 August, 2012, Beijing, China, pp213-221.

[9] Xiaoli Xiong, and Yongguang Hou, "Research on Detection and

Defense of Malicious Code under Network Security," International Journal of Network Security, vol.23, no.5, pp830-834, 2021.
[10] Kaifeng Jiang, Dongxu Shao, Stephane Bressan, Thomas Kister, and Kian-Lee Tan, "Publishing trajectories with differential privacy guarantees," Proceedings of the 25th International Conference on Science and Statistical Database Management, 29-31 July, 2013, Baltimore, MD, United states, pp1-12.
[11] Feng Tian, Shuangyue Zhang, Laifeng Lu, Hai Liu, and Xiaolin Gui, "A novel personalized differential privacy mechanism for trajectory data publication," Proceedings of the International Conference on Networking and Network Applications, 16-19 October, 2017, Kathmandu City, Nepal, pp61-68.
[12] Jingyu Hua, Yue Gao, and Sheng Zhong, "Differentially private publication of general time-serial trajectory data," Proceedings of the 34th IEEE Annual Conference on Computer Communications and Networks, 26 April-1May, 2015, Hong Kong, China, pp549-557.
[13] Meng Li, Liehuang Zhu, Zijian Zhang, and Rixin Xu, "Differentially private publication scheme for trajectory data," Proceedings of the 1st IEEE International Conference on Data Science in Cyberspace, 13-16 July, 2016, Changsha, Hunan, China, pp596-601.
[14] Si Chen, Anmin Fu, Mang Su, and Huaijiang Sun, "Trajectory privacy protection scheme based on differential privacy," Tongxin Xuebao, vol.42, no.9, pp54-64, 2021.
[15] Miguel E. Andrés, Nicolás E. Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi, "Geo-Indistinguish ability: differential privacy for location-based systems," Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, 4-8 November, 2013, Berlin, Germany, pp901-914.
[16] W.T. Chan, and K.S. Sim, "Termination Factor for Iterative Noise Reduction in MRI Images Using Histograms of Second-order Derivatives," IAENG International Journal of Computer Science, vol.48, no.1, pp174-180, 2021.