Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 12, No. 3, 2024

Secure and Efficient k-anonymous Trajectory Privacy Protection Method based on Differential Privacy

Yuanlong Fan[1, *], Cheng Song[2], Zhichao Wang[3]

[1] College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China
[2] College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China
[3] College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China
[*]Corresponding Author: Yuanlong Fan

Abstract: The Location-based service scheme have already involved in every aspect of People's daily life and are increasingly used in various industries. Aiming at the problem of the security and efficiency of mobile terminal users' trajectory privacy protection in location-based service, we propose a k-anonymous trajectory privacy protection scheme based on differential privacy. This scheme adopts differential privacy technology to add Laplace noise to the user's trajectory many times to generate 2k noise trajectory, and then according to the trajectory similarity to determine k-1 noise users whose trajectory are similar to the user trajectory, and sets them and the real user as an anonymous user group, and then uses the anonymous user group to request LBS services. Security analysis shows that the scheme satisfies the security features of anonymity, unforgeability, and anti-counterfeiting attack. The simulation results show that the scheme not only guarantees the similarity between the false trajectory and the real trajectory but also has higher execution efficiency.

Keywords: Mechanical engineering; Manufacturing technology; Electrical automation.

1. Introduction

With the development of mobile communication technology and location technology, LBS [1-3] is widely used in various fields, and users with mobile terminals can access information services anytime and anywhere, such as transportation, social communication, and emergency assistance[4].Users submit their geographic location and query information to location service providers to obtain some value-added services including points of interest [5].Although LBS has brought great convenience to users, it has also brought serious location privacy leakage problems to users. Location service providers collect users' location information and may sell this location information to third parties to gain benefits, or even leak the location information to malicious attackers. Malicious attackers use this location information to push ads or send spam messages to users, or even infer sensitive information such as users' residence address and workplace, which seriously violates users' privacy [6-7]. Therefore, how to protect users' trajectory privacy in location services is extremely important.

With the rapid development of location privacy protection technology, trajectory privacy protection technology has attracted extensive research attention from many domestic and foreign scholars. Based on anonymous generalization is an important approach to trajectory privacy protection. Li et al. [8] proposed fake trajectories are constructed by fully considering information such as background information, user action patterns and trajectory similarity to improve the confusion of fake trajectories and make it difficult for attackers to distinguish real trajectories from fake ones, but the communication between the client and the server may be eavesdropped by the attacker. Tian et al. [9] proposed an arc-tree (TPRT)-based scheme for storing and publishing differential privacy trajectory data is proposed. To preserve privacy, Laplacian noise is added to the sensitive counts of the radius tree and is constrained by Markov chains and privacy degrees. Many differential privacy based trajectory synthesis methods to publish trajectory data privately, but these methods do not adequately preserve the semantic information of the trajectories. Du et al. [10] proposed a semantic preservation scheme is proposed for synthesizing the trajectory data for publishing under differential privacy for this case. Many existing privacy-preserving publishing methods for trajectory data only provide the same level of privacy protection for all moving objects, while different moving objects may require different levels of privacy protection. Chen et al. [11] aiming at the shortcomings of the traditional k-anonymisation technique in which the value of δ is fixed and unchanged and no road network constraints are involved, the privacy preservation effect is improved by setting different thresholdsδat different road segments to generate the pseudo-trajectory dataset, but the efficiency is low.

Traditional approaches based on anonymity models, on the other hand, are difficult to protect against attackers that have a lot of information. Differential privacy protection approaches have become more popular in recent years for securing the privacy of moving object trajectories. Zhao et al. [12] proposed a trajectory privacy protection method for differential privacy clustering, which added constrained Laplacian noise to the trajectory position in the cluster to avoid excessive noise affecting the clustering effect and ensure the cluster analysis Data availability. This method improves data availability but reduces privacy. Chen et al. [13] proposed a dynamic trajectory privacy protection differential privacy scheme based on a recurrent neural network (RNN-DP), which introduced a recurrent neural network model to effectively process real-time data, but the efficiency was reduced. Ou et al. [14] considered that the correlation between the trajectories of two users may reveal sensitive social relationships, and proposed an n-body Laplacian framework that satisfies-differential privacy to prevent social relationship reasoning attacks. The scheme has good privacy and data

utility but does not consider the temporal correlations of trajectory.

To address the problem that the background knowledge of attackers cannot be effectively estimated in the current anonymous trajectory privacy protection, we propose a trajectory privacy protection scheme that combines anonymous and differential privacy techniques. In the scheme, the differential privacy technique is used to add Laplacian noise to the user's trajectory several times to generate noisy trajectories, and select multiple noisy users similar to the user's trajectory according to the trajectory similarity, set them and the real user as anonymous user groups, and use the anonymous user groups to request LBS services, so that the attacker cannot distinguish the real user from the noisy user, thus realizing the trajectory privacy protection for the user.

The rest of this paper is organized as follows: some necessary preliminaries are described in Sect. 2. The k-anonymous trajectory privacy protection scheme based on differential privacy is proposed in Sect. 3. The security analysis of the k-anonymous trajectory privacy protection scheme based on differential privacy is given in Sect. 4. Sect. 5 focuses on the simulation of the proposed scheme. And conclusions are drawn in Sect. 6.

2. Preliminaries

2.1. Systematic structure

As shown in Figure. 1, the trajectory privacy protection system model adopts an independent structure and consists of two parts: the client and the LBS server. The roles of each part are as follows:

Client: responsible for generating multiple noisy users, requesting the LBS server to obtain the query results, and completing the refinement of the query results.

LBS server: LBS responsible for receiving and processing the user's anonymization request, and returning the query result to the user.

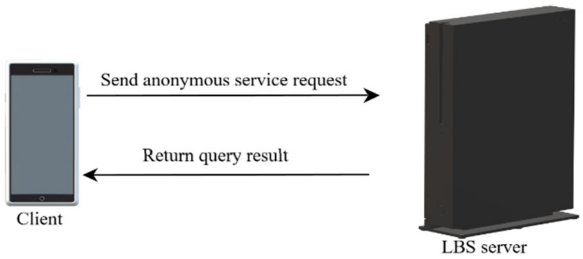

Figure 1. Architecture of location privacy protection system in this scheme

2.2. Trajectory similarity

Trajectory: Trajectory refers to the collection of the position sequence of a moving object at different moments, which can be expressed as:

$$T = \{id, (x_1, y_1, t_1), (x_2, y_2, t_2), \cdots, (x_n, y_n, t_n)\} \quad (1)$$

where id represents the identification of the moving object,represents the position of the moving object at the time (x_i, y_i), and (x_i, y_i, t_i) represents the number of positions on the trajectory.

Suppose that the movement direction of the user at the i position $L_i = (x_i, y_i)$ relative to the initial position is changed to,calculated between $L_i = (x_i, y_i)$ and $L_0 = (x_0, y_0)$ by $\theta_i = arctan\frac{y_i - y_0}{x_i - x_0}$. The position on the noise trajectory changes relative to the initial position xxx, so the trajectory similarity can be expressed as:

$$\delta^2 = \left(\frac{\sum_{i=1}^{n} \frac{\theta_i' - \theta_i}{2\pi}}{n}\right)^2 \quad (2)$$

The smaller δ^2 is, the more difficult it is to distinguish the user trajectory from the noise trajectory.

2.3. K-anonymity

K-anonymity is one of the privacy protection methods widely used in LBS location privacy protection. It provides low-precision privacy protection by generalizing and hiding certain attributes. Most location-based systems use k-anonymity to protect the identity of users, so that an attacker cannot determine which of the users is the real target. One method is to generate $k-1$ correct pseudo locations, and use the pseudo locations and real locations to form an anonymous user group to perform k queries to the location service provider. Another method is to create an invisible area containing k users who share points of interest, and then use this invisible area to query the server instead of the exact location. The larger the k, the lower the quality of service the user obtains, but the lower the risk of privacy leakage. However, when the attacker has enough background knowledge, he can infer the real target. Therefore, the differential privacy protection method that ignores background knowledge makes up for the shortcomings of k-anonymity in this respect.

2.4. Differential privacy

Differential privacy protection achieves the purpose of privacy protection by distorting data, ensuring that privacy leakage is minimized and data availability is maximized. Differential privacy is defined as follows:

ε -Differential Privacy [15-16]. Supposing that D_1 and D_2 are a pair of adjacent datasets that are only differ in one record, a random algorithm $\mathcal{A}$ is ε -differential private if of all S:

$$Pr[\mathcal{A}(D_1) \in S] \leq e^{\varepsilon} \times Pr[\mathcal{A}(D_2) \in S] \quad (3)$$

where Pr is the probability that the algorithm output and S is the subset of all the output of the algorithm $\mathcal{A}$.

Sensitivity. For the query function $\mathcal{F}: D \to R^d$, the sensitivity is defined as the difference between the adjacent datasets D_1 and D_2:

$$\Delta\mathcal{F} = max\|\mathcal{F}(D_1) - \mathcal{F}(D_2)\|_1 \quad (4)$$

Laplace mechanism [17]. The Laplace mechanism implements privacy protection by adding Laplacian distributed noise to the query results:

$$\mathcal{F}(D) + noise \quad (5)$$

The Laplace distribution density function is $\boldsymbol{f(x,\lambda)=\frac{e^{\frac{-|x-\mu|}{\lambda}}}{2\lambda}}$. Where $\boldsymbol{\mu}$ is expected value, for each noise, they are random variables drawn from the Laplace distribution centered at 0, that is, $\boldsymbol{\lambda=\frac{\Delta F}{\varepsilon}}$.

3. The proposed method

3.1. System Initialization

In this phase, system parameters are generated as follows:

Step 1**:** Define an elliptic curve $E(F_p): y^2 = x^3 + ax + b \bmod p$, Where p is a large prime number and F_p is a finite field of order large prime number p,$a, b \in F_p$,then select an additive group G of order q with generator P on the elliptic curve $E(F_p)$.

Step 2: The LBS server randomly selects a $s \in Z_q^*$ as the system key, and calculates its public key $P_{pub} = sP$, where Z_q^* is an integer multiplication group modulo q.

Step 3: Define three secure hash functions: $H_1: \{0,1\}^* \to Z_q^*$, $H_2: \{0,1\}^* \times G \to Z_q^*$, $H_3: \{0,1\}^* \times G \times G \times G \to Z_q^*$.

Step 4: LBS server publishes the public parameters of the system: $\text{params} = \{\text{a}, \text{b}, \text{p}, \text{q}, \text{P}, \text{G}, \text{P}_{\text{pub}}, \text{H}_1, \text{H}_2, \text{H}_3\}$, Secret system key: s.

3.2. User registration

Since this scheme is devised on the basis of k-anonymity, so in this phase, LBS server is employed to anonymize users' identities, which is as follows:

Step 1: User randomly selects a secret value $r_u \in Z_q^*$, and sends r_u and users real ID to LBS server to request registration.

Step 2: After receiving the registration request, the LBS server generates a false identity $PID_u = H_1(ID_u || r_u)$ for the user, then calculates $Q_u = H_2(PID_u, P_{pub})$, $J_u = Q_u P$, $S_u = Q_u + r_u s$, and returns the calculation result (PID_u, J_u, S_u) to the user through a secure channel.

Step 3: After receiving the message (PID_u, J_u, S_u), the user judges whether $S_u P \stackrel{?}{=} J_u + r_u P_{pub}$ is valid or not. If the equation is valid, randomly selects $\alpha_u \in Z_q^*$, calculates $b_u = H_2(PID_u, \alpha_u, params)$, $\beta_u = \alpha_u b_u$, $\rho_u = \beta_u P$, then use (α_u, β_u) as the private key and ρ_u as the public key; otherwise, go back to Step 1.

3.3. User registration

In this phase, false locations are generated from mobile terminal users, and $k-1$ optimal locations are selected from $2k$ false trajectorys. As follows:

Step 1: The Laplace cumulative distribution function is $F(x) = \int_{-\infty}^{x} Pr(x, \lambda)\, dx = 0.5\left[1 + sgn(x)(1 - exp(\frac{-|x|}{\lambda}))\right]$ and its inverse distribution function is $F^{-1}(x) = -\lambda \cdot sgn(p - 0.5) \cdot ln(1 - 2|p - 0.5|)$. where p is a random number of $[0,1]$, using the inverse distribution function to calculate the noise x that obeys the Laplace distribution.

Step 2: Define the user's trajectory as: $T_u = \{id_u, (x_1, y_1, t_i), (x_2, y_2, t_2), \cdots, (x_n, y_n, t_n)\}$, users adds Laplace noise to the real trajectory several times, that is, $\mathcal{F}(D) + x$, generating 2k noisy trajectories $T_{nt}^i = \{id_{nt}, (x_1^{nt}, y_1^{nt}, t_1^{nt}), (x_2^{nt}, y_2^{nt}, t_2^{nt}) \cdots, (x_n^{nt}, y_n^{nt}, t_n^{nt})\}$.

Step 3: The user calculates the trajectory similarity δ^2 between the real and noisy trajectories by the trajectory similarity formula $\delta^2 = \left(\frac{\sum_{i=1}^{n} \frac{\theta_i' - \theta_i}{2\pi}}{n}\right)^2$.

Step 4: The user filters out the top $k-1$ trajectories with high similarity according to parameter k, corresponding to $k-1$ noisy users respectively.

Step 5: The $k-1$ noise users are registered separately and the LBS server generates an anonymous identity $PID_i (1 \le i \le k-1)$ and the corresponding public and private keys for each noise user.

Step 6: The user and the $k-1$ noise users together form the k anonymous user group, which requests the LBS service.

3.4. Location service request

In this phase, mobile terminal user randomly selects one user as representative to send service request to LBS server. The steps are as follows:

Step 1: User randomly selects one user from the k anonymous user group as the representative user pu. The private key of the representative user is$(\alpha_{pu}, \beta_{pu})$,the public key is ρ_{pu}, $r_{pu} \in Z_q^*$ is randomly selected when a representative user registers, $(PID_{pu}, J_{pu}, S_{pu})$ is the message returned from the LBS server during registration, msg is the request message.

Step 2: Representative user randomly selects $\omega_{pu} \in Z_q^*$ and current time stamp t_{pu}, and calculates $R_{pu} = \omega_{pu}\alpha_{pu}P$, $h_{pu} = H_3(R_{pu}, msg, t_{pu}, \rho_{pu}, PID_{pu})$ and $\sigma_{pu} = \omega_{pu}\alpha_{pu} + h_{pu}\beta_{pu} + S_{pu}$.After this (σ_{pu}, R_{pu}) and msg are sent to the LBS server.

Step 3: After receiving (σ_{pu}, R_{pu}) and msg, LBS server verifies that the timestamp t_{pu} is fresh, if so, proceed to the next step; otherwise, go back to Step 1.

Step 4: The LBS server calculates $h_{pu} = H_3(R_{pu}, msg, t_{pu}, \rho_{pu}, PID_{pu})$, then judges whether the equation $\sigma_{pu}P \stackrel{?}{=} R_{pu} + h_{pu}\rho_{pu} + J_{pu} + r_{pu}P_{pub}$ is valid or not. If the equation is valid, LBS server returns the query result set $Rres = \{r_{res}1, r_{res}2, \cdots, r_{res}k\}$ to user; otherwise, refuses to return the query result set.

Step 5: After receiving $Rres$, user selects from them the required real message $r_{res}u$.

4. Security Analysis

4.1. Anonymity

Anonymous game. If the attacker A wins the anonymous game with negligible probability in polynomial time, the scheme satisfies the anonymity. Anonymous game is descried as follows:

Step 1: Challenger C provided system parameters $\{a, b, p, q, P, G, P_{pub}, H_1, H_2, H_3\}$ to attacker A.

Step 2: Attacker A chooses two different messages m_0, m_1.

Step 3: Challenger C randomly selects $b \in \{0,1\}$, b keeps the attacker A secret. Then send m_b and m_{1-b} to two users U_0 and U_1.

Step 4: Users U_0 and U_1 construct signatures (σ_b, R_b) and (σ_{1-b}, R_{1-b}) based on m_b and m_{1-b}, respectively.

Step 5: If the signatures (σ_b, R_b) and (σ_{1-b}, R_{1-b}) generated by U_0 and U2 correspond to the messages m_b and m_{1-b}.

Step 6: Attacker A outputs $b' \in \{0,1\}$ as a guess for b, if $b' = b$, attacker A wins the anonymous game.

Proof: The user identity is encrypted with a hash function during the registration process to generate a fake identity $PID_u = H_1(ID_u||r_u)$, due to the one-way nature of the hash function, it is difficult for the attacker A to infer the real identity of the user from the PID_u. At the same time, if the attacker tries to obtain the user's private information through the message (σ_{pu}, R_{pu}), then s must be solved by $P_{\text{pub}} = sP$ and solved (α_u, β_u) by $\beta_u = \alpha_u b_u$ and $\rho_u = \beta_u P$, that is, the attacker must obtain the system key s, the user's private key (α_u, β_u) and a random number r_u. Solving the above problem is faced with the difficult problem of solving the discrete logarithm of elliptic curve. It is computationally infeasible, so the advantage of attacker A to win the game $Adv(A) = |Pr(b = b') - \frac{1}{2}|$ is negligible, that is, the solution satisfies anonymity.

4.2. Unforgeability

In the random oracle model (ROM), if the attacker A is unable to fake the LBS server to forge user registration information in polynomial time, the solution meets the unforgeability. The following is the proof:

Proof: Assuming that the attacker A can forge the user registration information with a non-negligible probability in polynomial time, that is, the attacker A can calculate the system key s with a non-negligible probability in polynomial time, and finally the equation $S_u P = J_u + r_u P_{pub}$ is established.

Setup: Challenger C performs system initialization, sends system public parameters to attacker A, and runs a key generation algorithm to generate the sender's public-private key pair (PK_u, SK_u), and sends the public key PK_u to attacker A.

Query: Attacker A performs a polynomial bounded sub-adaptive oracle query. The following shows the type of query of attacker A.

1) Hash query: Attacker A performs a hash value query, and challenger C returns the relative hash value to attacker A.

2) Private key extraction query: Attacker A selects an attribute set pro_i according to his needs, and asks challenger C for the private key of the corresponding user. Challenger C generates a public-private key pair (TKi, SK_{pro_i}) according to the key generation algorithm, and sends (TKi, SK_{pro_i}) to attacker A.

3) Signature query: The attacker A asks the challenger C for the signature of the message M under the attribute set pro_i and the receiver attribute set rec_i. The challenger C runs the signature algorithm, generates the corresponding signature σ and returns it to the attacker A.

4) Verification query: After receiving the signature σ and the message m from the attacker A, the challenger C runs the verification algorithm. If the verification is successful, it returns $true$; otherwise, it returns $false$.

Challenge: Attacker A generates a signature σ^* with attribute set pro' and receiver attribute rec_j. If the verification query result of is not $false$ and (m, pro', rec_j) is not asked by the signature, attacker A wins the unforgeable game.

Guess: Attacker A fakes a trusted anonymous server to forge user registration information. During the inquiry process, because attacker A cannot obtain the system master key s, the equation $S_u P = J_u + r_u P_{pub}$ cannot be established. If the attacker A tries to obtain the system master key, he needs to derive the private key s through the equation $P_{pub} = sP$. The solving problem is equivalent to solving the elliptic curve discrete logarithm problem, that is, the attacker A cannot be in polynomial time. Ignore the probability to solve the elliptic curve discrete logarithm problem. Therefore, the scheme satisfies unforgeability.

4.3. Resistance of impersonation attack

On the premise of solution of the elliptic curve discrete logarithm problem (ECDLP) is difficult, attacker A cannot impersonate a user to send a signature in polynomial time, that is, the scheme is resistant to impersonation attacks. The following is the proof:

Proof: If the attacker A tries to impersonate the user and send the signature to the LBS server successfully in polynomial time, he needs to confirm to the LBS server that the equation holds, that is, the attacker must know the and the system master key. To obtain the and the system master key, the attacker A needs to obtain the random number and the user private key, and solve the according to. Because and keep the attacker A secret, solving is equivalent to solving the elliptic curve discrete logarithm problem. Therefore, the program is resistant to impersonation attacks.

5. Analysis on Trajectory Similarity

The environment of simulation experiment is Intel i9-13900HX 2.20 GHz CPU, 16 GB RAM, Windows 11 operation system, MATLAB simulation software and moving object generator Thomas Brinkhoff environment. Generate a large number of trajectory data of moving objects through Thomas Brinkhoff, randomly select a moving object, generate $2k$ noise trajectories through the Laplacian noise algorithm, and select $k-1$ noise trajectories according to the trajectory similarity algorithm to achieve real trajectory $k$anonymity.

5.1. Anonymity

The trajectory similarity reflects the trajectory privacy protection effect to a certain extent. The smaller the trajectory similarity is, the better the trajectory privacy protection effect is. The simulation experiment selects , as shown in Figure. 2, with the increase of , the trajectory similarity of this scheme and the comparison scheme changes little. Ref. [8] considers the characteristics of user behavior patterns and trajectory similarity. According to the background information of the user's area, a false trajectory is constructed by methods such as trajectory rotation, which can effectively resist background knowledge attacks, and the trajectory similarity is relatively small. Ref. [11] scheme considers the road network information when generating the virtual position and generates the pseudo-position based on the road network threshold set, and the generated pseudo-trajectory has high trajectory similarity with the real trajectory. The scheme proposed in this paper generates noise trajectories by adding Laplacian noise to user trajectories multiple times, and selects the first noise trajectories with less similarity according to the trajectory similarity formula, and discards the ones with greater trajectories similarity. Noisy trajectories, so this scheme has the lowest trajectory similarity.

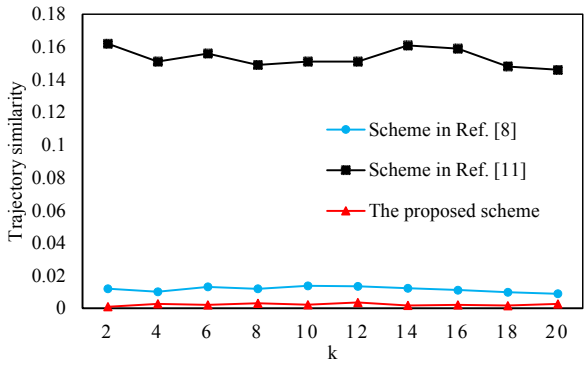

Figure 2. The relationship between k and trajectory similarity

5.2. Anonymity

In the case of a certain differential budget ε, the relation between the algorithm execution time and k of the three schemes is shown in Figure. 3. Ref. [8] considers multiple factors such as user behavior patterns, generates false trajectories through trajectory rotation, and needs to traverse the values at each time point corresponding to the false trajectories to perform corresponding offsets, and the algorithm execution time is long. Ref.[11] firstly constructs an adaptive threshold set according to the road network information; then, the network topology map of the road network is used as a motion model to generate virtual trajectories, and the execution time of the scheme is relatively high due to the need to take into account the influence of the road network constraints when the scheme generates virtual trajectories. This scheme just adds noise to the existing trajectory and selects the $k-1$ noise trajectory through the trajectory similarity formula, without considering other factors, and the algorithm has the highest execution efficiency.

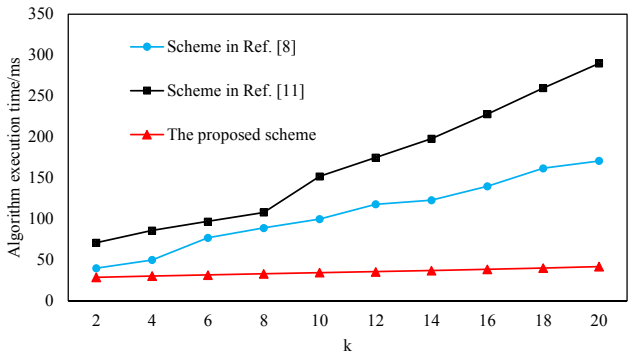

Figure 3. The relation between k and algorithm execution time

The relationship between k and ε and the algorithm execution time is shown in Figure. 4. When ε is constant, the execution time of the algorithm increases with the increase of k; when k is constant, the execution time of the algorithm changes little with the increase of ε. When $k=5$, with the increase of ε, the execution time of the algorithm fluctuates around 30ms. When $k=10$, with the increase of ε, the execution time of the algorithm fluctuates around 35ms. When $k=15$, with the increase of ε, the execution time of the algorithm fluctuates around 38ms. Because ε affects the size of the noise, and the size of the noise has little effect on the execution time of the algorithm, ε has basically no effect on the execution time of the algorithm.

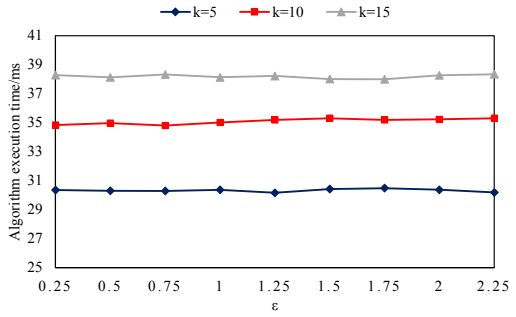

Figure 3. Influence of k and ε on the algorithm execution time

6. Analysis on Trajectory Similarity

Aiming at the security and efficiency of mobile terminal user trajectory privacy protection in location based services, a trajectory privacy protection scheme combining anonymity and differential privacy technology is proposed. Based on the anonymity of user identity, the scheme uses differential privacy mechanism to add Laplacian noise to user trajectories multiple times to generate noise trajectories, and selects noise users similar to user trajectories according to the trajectory similarity. The noise users and real users are set as the anonymous user group, and the LBS service is requested as the anonymous user group, so as to protect the privacy of user trajectories and ensure the service quality of LBS users. Through security analysis, the scheme satisfies the security features such as anonymity, unforgeability and resistant to impersonation attack. Finally, simulation experiments are carried out on the scheme from the aspects of trajectory similarity and efficiency. The results show that the scheme is superior to other schemes in terms of trajectory similarity and algorithm execution time. Therefore, the proposed scheme has certain theoretical significance and application value in trajectory privacy protection.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61872126, 62273290); the Science and Technology Research Program of Henan Province (212102210092, 222102210078)

References

[1] Qiu G, Tang G, Li C, et al. Differentiated Location Privacy Protection in Mobile Communication Services: A Survey from the Semantic Perception Perspective[J]. ACM Computing Surveys, 2023, 56(3): 1-36.

[2] Zhang S, Li M, Liang W, et al. A Survey of Dummy-Based Location Privacy Protection Techniques for Location-Based Services[J]. Sensors, 2022, 22(16): 6141.

[3] Jiang H, Li J, Zhao P, et al. Location privacy-preserving mechanisms in location-based services: A comprehensive survey[J]. ACM Computing Surveys (CSUR), 2021, 54(1): 1-36.

[4] Cheng S, Daochen C, Shuiping N I. k Anonymous Trajectory Privacy Protection Scheme of Personalized Differential Privacy[J]. Journal of Beijing University of Posts and Telecommunications, 2023, 46(3): 109.

[5] Sánchez P, Bellogín A. Point-of-interest recommender systems based on location-based social networks: a survey from an

experimental perspective[J]. ACM Computing Surveys (CSUR), 2022, 54(11s): 1-37.

[6] Mariana C, Ricardo M, Vilela JP. A survey of privacy-preserving mechanisms for heterogeneous data types. Computer Science Review, 2021, 41: 15p.

[7] Wazirali R. A Review on Privacy Preservation of Location-Based Services in Internet of Thing. Intelligent Automation and Soft Computing, 2022, 31(2): 767-779.

[8] Li F H, Zhang C, Niu B, et al. Efficient scheme for user's trajectory privacy[J]. Journal on Communications, 2015, 36(12): 114-123.

[9] Tian J, Zhu Q. A differential privacy trajectory data storage and publishing scheme based on radix tree[J]. Concurrency and Computation: Practice and Experience, 2023: e7731.

[10] Du X, Zhu H, Zheng Y, et al. A Semantic-Preserving Scheme to Trajectory Synthesis Using Differential Privacy[J]. IEEE Internet of Things Journal, 2023.

[11] H. Chen, S. Li and Z. Zhang, "A differential privacy based (k-Ψ)-anonymity method for trajectory data publishing," Computers, Materials & Continua, vol. 65, no.3, pp. 2665–2685, 2020.

[12] Zhao X, Pi D, Chen J. Novel trajectory privacy-preserving method based on clustering using differential privacy[J]. Expert Systems with Applications, 2020, 149: 113241.

[13] Chen S, Fu A, Shen J, et al. RNN-DP: A new differential privacy scheme base on Recurrent Neural Network for Dynamic trajectory privacy protection[J]. Journal of Network and Computer Applications, 2020, 168: 102736.

[14] Ou L, Qin Z, Liao S, et al. Releasing correlated trajectories: Towards high utility and optimal differential privacy[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 17(5): 1109-1123.

[15] Shang T, Zhao Z, Ren X, et al. Differential identifiability clustering algorithms for big data analysis[J]. Science China Information Sciences, 2021, 64: 1-18.

[16] Dwork C, Roth A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2014, 9(3–4): 211-407.

[17] Fernandes N, McIver A, Morgan C. The Laplace Mechanism has optimal utility for differential privacy over continuous queries[C]//2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). IEEE, 2021: 1-12.