Journal of Information Hiding and Multimedia Signal Processing ©2019 ISSN 2073-4212
Ubiquitous International Volume **10**, Number **2**, March **2019**

A Trajectory Privacy Protection Scheme based on DTW Switch Query in Location-based Services

Cheng Song, Yadong Zhang*, Xixi Yan and Zhizhong Liu

School of Computer Science and Technology
Henan Polytechnic University
Jiaozuo, Henan, 454000, China
*Corresponding author:18339161026@163.com

Received July 2018; revised October 2018

Abstract. *To solve the problem of private location information leak due to the aggressive inference of trajectory data from continuous location-based services (LBS) query, a trajectory privacy protection scheme based on DTW switch query is put forward. In this scheme, the identities of user and candidates who request LBS are anonymized, then DTW algorithm is adopted to successively calculate the trajectory similarities between all candidates and initiator at certain time intervals, from which candidate with optimal trajectory similarity is selected to represent real users in requesting LBS, so as to protect user identity and location. Security analyses prove that the scheme is not only able to guarantee such security features as anonymity in the random oracle model and non-forgeability, but also able to resist continuous query tracing attack. And the results of simulation experiment show that the similarity of the optimal candidate trajectory in this scheme is remarkably improved.*

Keywords: LBS; DTW; Trajectory privacy protection; Switch query

1. **Introduction.** Along with the rapid development of wireless communications technology, Global Position System (GPS) and intelligent mobile terminals, users are able to get access to the conveniences of location-based services (LBS) [1-3] anywhere and anytime, such as location, navigation, query, identification, event checking, etc. Although, location-based services bring a lot of conveniences to peoples daily life, they also increase the risk of users' privacy disclosure. For example, in LBS request, when mobile terminal users information like location, ID and query is usually transmitted in plain text to be processed by location information server, these private information[4] will take the risk of being leaked if being intercepted or monitored by attackers, which may further cause some threat to users. At present, in the location-based services, the user's location privacy can be roughly divided into two categories: one is snapshot query location privacy, that is, the single-point location privacy when the user initiates the location query service at a certain moment. The other is the trajectory privacy when the user initiates the query continuously in a period of time. Despite some progress has been made in preventing users from leaking private information at a single point [5-7], researchers are still aware that only securing users location information is not enough to guarantee users privacy, for if attackers construct location trajectories based on spatiotemporal relevancy, then they can acquire users relevant privacy information by analyzing those trajectories. Therefore, while protecting users location privacy, how to effectively prevent the leak of users trajectory information proves to be an urgent problem to be solved [8].

Aiming to address the deficiencies in the existing schemes while take advantage of their merits, we propose a trajectory privacy protection scheme based on DTW switch query. In this scheme, the identities of all candidates and user requesting LBS are anonymizied to hide their real identities, then DTW algorithm is adopted to successively calculate the trajectory similarities between all candidates and user at certain time intervals, from which the candidate with optimal trajectory similarity is selected to represent real user in requesting LBS. Since the optimal candidates that represent users in requesting LBS are different at different time intervals in user mobility trajectory, the attacker is unable to infer the relevancy via the intersection of user sets in cloak area at different time intervals. In this way, the privacy protection of user mobility trajectory can be fully guaranteed. The following summarizes the main contributions of this paper:

1. We propose a trajectory privacy protection scheme based on DTW switch query. In this scheme, the real user exchanges the LBS service query with the optimal candidate to realize the confusion of the trajectory, thereby achieving the purpose of protecting the privacy of the real user trajectory.

2. Through anonymizing the identities of user and candidates who request LBS, and calculating the trajectory similarity between all candidates and the initiator within a certain period of time by using the DTW algorithm, then choosing the candidate with the optimal trajectory similarity to replace real user in requesting LBS, the real users private information about identity and location is effectively protected.

3. We conduct security analyses of the proposed solution. Security analyses prove that the scheme is able to guarantee such security features as anonymity in the random oracle model, non-forgeability and to resist continuous query tracing attack. And the results of simulation experiment show that the similarity of the optimal candidate trajectory in this scheme is remarkably improved.

The rest of this paper is organized as follows: In section 1, we show the Introduction. In section 2, we introduce the related work. In section 3, we introduce the preliminaries. The trajectory privacy protection scheme is described in detail in section 4. We offer the security analyses in section 5. In section 6, we give the simulation experiment about the similarity of the optimal candidates trajectory. The conclusions are given in section 7.

2. **Related work.** In the last few years, some researchers home and abroad have done lots of research in view of protecting mobile terminal users trajectory privacy. Gruteser et al. [9] in 2004 differentiated sensitive areas from non-sensitive areas on the basis of the amount of objectives in these areas, so as to protect trajectory privacy by restraining or deferring users location update in sensitive areas. Terrovitis et al.[10] in 2008 adopted iterative restraint method to select from the trajectories the locations that could realize privacy constraints. Nevertheless, the restrained trajectories may lead to the damage of massive information, thus weakening service quality. In Reference [11], a partial suppression scheme for a tailored privacy model was proposed to realize privacy preservation of trajectory data, so as to reduce the information damage. Zhao et al. [12] proposed a privacy protection approach based on trajectory frequency suppression, in which the privacy is protected by adding fake data to defective trajectory data or partial suppression. Lei et al. [13] argued that the key of trajectory privacy preservation is how to generate dummy trajectory. Later, Dai et al. [14] proposed a dummy trajectory generation scheme based on the segmented fake trajectory, in which, the fake positions are generated for the sampling locations of real trajectories at different time points, and the segmented fake trajectories are generated at different time intervals. In fact, these schemes are all based on the idea of dummy trajectory fuzzification and suppression, which, although simple in realization and high in efficiency, is relatively low in privacy degree. Chow et al. [15]

put forward a K-anonymized district-sharing scheme, in which, by querying $k-1$ similar users along with the real user in continuous query, LBS server fails to identify the real user. Huo et al. [16] reduced information loss by employing greedy partition graph to select trajectory anonymity sets. Kato et al. [17] assumed that users' movements are known in advance, and on the basis of users mobility trajectories and pauses, selected each hop of dummy trajectories according to the deviation angles of users locations and accessibility. Finally they proposed a dummy-based anonymization scheme for trajectory privacy protection. However, this scheme has no preferred similarity. Hwang et al. [18] devised a comprehensive trajectory privacy technique based on users privacy profiles, in which a set of similar trajectories are preprocessed to blur users actual trajectories, and a novel time-obfuscated technique is introduced. Due to the massive calculation required by each preprocessing, the efficiency in this scheme turns out to be low. Schlege et al. [19] proposed a user-defined privacy grid system, which fulfills the basic requirements for privacy-preserving snapshot and continuous LBS, but still requires a third-party.

3. Preliminaries.

3.1. **System model of trajectory privacy protection.** As is shown in Figure 1, the system model of trajectory privacy protection is mainly composed of three entities: mobile terminal, trusted anonymous server (TAS) and LBS server. The functions of each entity are as follows:

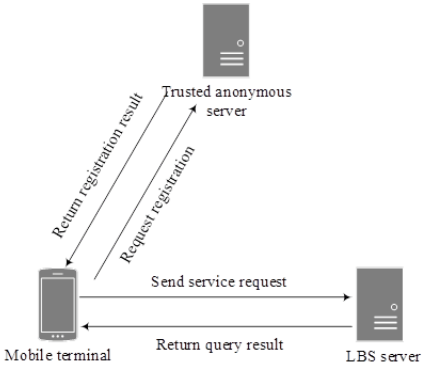

Figure 1. System model of location privacy protection

(1) Mobile terminal: on the one hand, mobile terminal sends request for anonymization to anonymous server and verifies the validity of the anonymity; on the other hand, it sends location query request, and receives query result from the server.

(2) Trusted anonymous server: a trusted anonymous server is required to be equipped in anonymity location privacy protection so as to preserve the registered users information of attribute matrix, receive request from mobile terminal, identify the optimal user with the most similar trajectory for mobile terminal, and release system parameters.

(3) LBS server: as the core of location privacy protection system, it is responsible for processing anonymity query from mobile terminal and returning query results to the terminal.

3.2. **Trajectory data set.** For any moving object A, its moving trajectory T_A is composed of a set of discrete positions within sampling time, while trajectory data set T is the set of all users trajectory sequences, which is represented as:$T=\{T_k\}, k=1,2,\cdots$ (T_k is the motion trajectory of user i). The motion trajectory T_k of each user k is composed of n location sequences at different time intervals t_i, represented as: $T_k=\{ID_K,(x_1,y_1,t_1),(x_2,$

$y_2, t_2), \cdots, (x_n, y_n, t_n)\}$. In this equation, $(t_1 < t_2 < \cdots < t_n)$, ID_i stands for users anonymous identities, (x_i, y_i) the objects location at time intervals t_i, and t_i the sampling time.

3.3. Dynamic Time Warping Algorithm.

Dynamic Time Warping (DTW) algorithm is designed in view of the excessively rigorous requirements for sampling in traditional algorithms. It calculates the minimum distance as the similarity measure of the trajectories by adopting the recording points prior to the repetition to complement the corresponding vacancies. Let sequence $L = \{l_1, l_2, l_3, \cdots, l_m\}$ and sequence $H = \{h_1, h_2, h_3, \cdots, h_n\}$ respectively represents the discrete spatial sampling of two trajectories, in which $m > 1$, $n > 1$. In order to align the elements of L with those of H, a matrix $m \times n$ is constructed, and the elements of the matrix (i, j) respectively represent the Euclidean distance $Dist(l_i, h_j)$ between the two points l_i and h_j. The similarity of two trajectories is represented as: $DTW(L, H) = D(m, n)$, in which $D(m, n)$ satisfies

$$D(i,j) = Dist(i,j) + min\begin{cases} D(i, j-1) \\ D(i-1, j) \\ D(i-1, j-1) \end{cases} \tag{1}$$

In this equation, $D(i, j)$ stands for the warping path distance between sequences L and H.

4. Trajectory Privacy Protection Scheme Based on DTW Switch Query.

4.1. System Initialization.

In this phase, system parameters are generated as follows:

Step 1: Let G_1 and G_2 be the cyclic groups of prime order q, G_1 be the addition cyclic group, G_2 be the multiplication cyclic group, P be a generator of G_1 . $e : G_1 \times G_1 \rightarrow G_2$ represents a bilinear map[20], and Z_q^* is the integer multiplication group of mode q .

Step 2: Define three secure harsh functions: $H_1 : \{0,1\}^* \rightarrow G_1^*$, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^k$, and $H_3 : G_2 \rightarrow \{0,1\}^n$, where $\{0,1\}^*$ stands for binary strings of arbitrary length, and k is an integer.

Step 3: TAS selects master key $s \in Z_q^*$ and $\gamma \in G_1^*$ for the system , and calculates its public key: $PK_{anon} = sP$ and private key: $SK_{anon} = s\gamma$.

Step 4: TAS publicizes system parameter: $\{G_1, G_2, e, k, n, P, P_{anon}, H_1, H_2, H_3\}$.

4.2. Registration.

In this phase, users identity is anonymized via TAS, and the corresponding parameters are generated, as follows:

Step 1: Mobile terminal sends its real identity ID to TAS as registration request message.

Step 2: TAS randomly generates a $m \times n$ matrix $Z(2 \leq m < n)$ and a m-dimensional column vector p, satisfies $R(Z) = R(\bar{Z})$ and $R(Z) < n$, that is, linear equation $Zd = p$ has infinite solutions.

Step 3: TAS generates a unique n -dimensional column vector d_i for each user requesting registration, and satisfies $Zd_i = p$, that is, d_i is one solution of linear equation $Zd_i = p$. TAS randomly selects a n-dimensional column vector D and generates the salt value ID_{salty} by using the pseudo random number generator based on encryption. calculates the false identities $PID_u = D^T \bullet d_u \bullet ID_{salty}$, $Q_u = H(PID_u)$ and $X_u = sQ_u$ of user U, and returns $\{PID_u, X_u, d_u\}$ to user U via secure channel.

Step 4: After receiving message $\{PID_u, X_u, d_u\}$, user u calculates $\tilde{Q} = H_1(PID_u)$ and judges whether $e(X_u, P) = e(\tilde{Q}_u, PK_{anon})$ is valid or not. If the equation is valid, user u adopts X_u as part of its private key, and randomly selects a secret value $r_u \in Z_q^*$, calculates its private key $SK_u = r_u X_u$ and public key $PK_u = r_u PK_{anon}$; f not valid, return to Step 1.

4.3. **Calculation of Trajectory Similarity of DTW.** Assume $L_u = \{l_1, l_2, l_3, \ldots, l_m\}$ and $H_c = \{h_1, h_2, h_3, \ldots, h_n\}$ respectively represents the discrete spatial sampling of initiators and candidates motion trajectories, in which $m > 1$, $n > 1$. Anonymous server adopts DTW algorithm to calculate successively the trajectory similarity of the initiator and the candidate. As follows:

Step 1: According to the Euclidean distance between sequence points L_u and H_c , a sequence distance matrix $M_{m\times n}$ is generated, in which the row corresponds with sequence L_u, and the column corresponds with sequence H_c, and the matrix element is the Euclidean distance between sequence points L_u and L_u.

Step 2: Based on matrix $M_{m\times n}$, loss matrix M_c is generated. The calculation method is: the first row and the first column of M_c are the elements of the first row and first column in matrix $M_{m\times n}$. Through $M_c(i,j) = Min\{M_c(i-1,j), M_c(i-1,j-1), M_c(i,j-1)\}+ M(i,j)$, calculates successively the value of elements $M_c(i,j)$ in other locations. The elements in the last row and last column of the loss matrix M_c are the distance between sequence points L_u and H_c, that is, the trajectory similarity.

Step 3: Likewise, calculates separately the similarity between real trajectory and other candidate trajectories within the same time intervals Δt.

4.4. **Location Service Request for Switch Query.** In this phase, TAS finds for user a candidate user whose trajectory is the most similar to user u at certain time interval. The specific service request is as follows:

Step 1: Mobile terminal u launches broadcast, obtains the anonymous identity $m_1 = \{ PID_C^1, PID_C^2, \ldots, PID_C^{k-1}\}$ of candidate user in certain region. Mobile terminal u randomly selects $\omega \in Z_q^*$, to calculates $Q_{LBS} = H_1(ID_{LBS})$, $c_1 = \{\omega p, m_1 \oplus H_3(e(Q, PK_{anon})^{\omega})\}$=$\{E, F\}$ and $c_2 = \{\omega p, m_2 \oplus H_3(e(Q_{LBS}, PK_{LBS})^{\omega})\}$=$\{E, F\}$, where ID_{LBS} represents the identity of LBS server, $m_2 = \{L_u, M_u, K_s\}$, PK_{LBS} is the public key of LBS server, L_u is the location, M_u is the content of query, and K_s is the session key of user and LBS server.

Step 2: Receiving the request, the TAS randomly selects $i \in Z_q^*$, calculates and verifies parameter I and $r : I = iZ$ and $r = ip$, then sends the verification message $\{t_1, I, H_2(r||ID_{Tu}||t_1)\}$ to the mobile terminal user u, in which ID_{Tu} is the identification of TAS, and t_1 is the time stamp.

Step 3: After receiving the message from TAS, user u firstly calculates $R = id_i$, then verifies the equation $H_2(R||ID_{Tu}||t_1) = H_2(r||ID_{Tu}||t_1)$. If the equation is valid, calculates $\{t_2, H_2 = (R||ID_{Tu}||t_1||t_2)\}$, and sends it to TAS, in which t_2 is the time stamp.

Step 4: Receiving the message, TAS verifies the equation $H_2(R||ID_{Tu}||t_1||t_2) = H_2(r||ID_{Tu}||t_1||t_2)$. If valid, calculate $F \oplus H_3(e(SK_{anon}, E))$, that is, get the message m_1, and extract all candidates attribute information according to the message m_1 ; then select the optimal candidate B within a certain time interval based on the result of calculating the trajectory similarity of similar trajectory algorithm. TAS randomly selects $\beta \in Z_q^*$ calculates $Q_B = H_1(PID_B)$ and $c_3 = \{\beta P, m_3 \oplus H_3(e(Q_B, PK_B)^{\beta})\}$ in which PK_B is the public key of candidate B and $m_3 = \{PID_u\}$; finally sends data packet $Meg_{NoB} = \{c_2, c_3\}$ to candidate B, and B represents user U to initiate LBS request.

Step 5: Receiving the message, user B calculates $\{m_3 \oplus H_3(e(Q_B, PK_B)^{\beta}) \oplus H_3(e(SK_B ,\beta P))\}$ to get the message m_3, where $SK_B = r_B s Q_B$ is the private key of user B, then sends $Meg_{BoS} = \{c_2\}$ to LBS server.

Step 6: Receiving the data packet, LBS server calculates $m_2 \oplus H_3(e(Q_{LBS}, PK_{LBS})^{\omega}) \oplus H_3(e(SK_{LBS}, \omega P))$ to get the message m_2, then the query request result $m_4 = \{MEG\}$ is obtained according to the m_2, and finally send the packet $Meg_{SoB} = \{En_{K_s}(m_4)\}$ to the user , in which $En_K()$ is the encrypted symmetric function and MEG is the result of the request of the LBS service query.

Step 7: Receiving the message $Meg_{SoB} = \{En_{K_s}(m_4)\}$, user B verifies the identity of user . If the identity is valid, sends $Meg_{Bou} = \{En_{K_s}(m_4)\}$ to user u; otherwise, cease the service.

Step 8: After receiving the message, user u decrypts $Meg_{Bou} = \{En_{K_s}(m_4)\}$, and obtains the query result MEG .

5. Security Analysis.

This scheme conducts security analyses in terms of three aspects: anonymity, non-forgeability and resistance to query tracing attack.

5.1. Anonymity.

Definition 1: Anonymity game.

Step 1: The attacker launches query, then obtains the public parameters of the system:$\{G_1, G_2, e, k, n, P, P_{anon}, H_1, H_2, H_3\}$, and the necessary information of the parameters;

Step 2: The attacker selects two totally different encryption messages m_0 and m_1;

Step 3: Selects random bit $b \in \{0, 1\}$, then sends m_b and m_{1-b} to two optimal candidates u_1 and u_2, b is confidential to the attacker;

Step 4: The TAS searches for the best candidate B_0 and B_1 for u_1 and u_2, and sends the encrypted identity information c_b and c_{1-b} to B_0 and B_1.

Step 5: If B_0 and B_1 receive encrypted information c_b and c_{1-b} correspond to information m_b and m_{1-b} respectively, then sends c_b and c_{1-b} to the attacker in random order; otherwise, return $\perp$ to the attacker;

Step 6: If the attacker A decrypts c_b , it can output the message $m'_b = m_b$, then he wins the game. This article assumes the advantage of attacker winning this game as: $Adv(A) = |Pr[A]|$, in which $PA[A]$ means that attacker A can output the probability of $m'_b = m_b$.

Theorem 5.1. *In the trajectory privacy protection scheme, assume attacker A wins the anonymity game with negligible probability, then this scheme satisfies the requirement for anonymity.*

Proof: Assume attacker A as the attacker in the anonymity game in Definition 1, if $\perp$ is returned in Step 5, then attacker A is unable to obtain any useful information. Then consider another possibility: assume attacker A obtains two encrypted results of the request query, that is: $M_{NoB_0} = \{c_b\}, M_{NoB_1} = \{c_{1-b}\}$. Where $c_b = \{\nu P, m_b \oplus H_3(Q_{B_0}, PK_{B_0})^\nu\}$, $c_{1-b} = \{\zeta P, m_{1-b} \oplus H_3(Q_{B_1}, PK_{B_1})^\zeta\}$, in which $\nu \in Z_q^*$ and $\zeta \in Z_q^*$ stand for two random numbers generated by TAS . PK_{B_0} and PK_{B_1} are the public keys of user B_0 and B_1 . Assuming the attacker's private key is $SK_{Attack} = r_{Attack} s_{Attack} Q_{ATttack}$. If the attacker tries to get the user's identity information m_b by decrypting $c_b = \{\nu P, m_b \oplus H_3(Q_{B_0}, PK_{B_0})^\nu\}$, he has to solve $H_3(Q_{B_0}, PK_{B_0})^\nu$. Bacause Q_{B_0} and PK_{B_0} are known, the attacker can let $Q_{Attack} = Q_{B_0}$, $r_{Attack} s_{Attack} P = PK_{B_0}$ and calculate $H_3(e(Q_{Attack}, r_{Attack} s_{Attack} P)^{\nu'})$. If the attacker wants to succeed, the equation $H_3(e(Q_{Attack}, r_{Attack} s_{Attack} P)^{\nu'}) = H_3(e(Q_{B_0}, PK_{B_0})^\nu)$ must hold, that means $\nu' = \nu$. The random number ν satisfies equation $\lambda_b = \nu P$. The difficulty of the attacker obtaining the random number ν is equivalent to solving the elliptic curve discrete logarithm problem, which is not feasible in computation. The attacker winning the game is negligible in Probability, so the scheme satisfies anonymity.

5.2. Non-forgeability.

Theorem 5.2. *In Random Oracle Model (ROM), if attacker F exists to forge users registration information by masquerading TAS in polynomial time, then Diffie-Hellman, the calculative problem, can be solved with non-negligible probability in polynomial time.*

Proof: Assume attacker F is able to solve the calculative problem Diffie-Hellman with non-negligible probability in polynomial time, that is, attacker F finds s with non-negligible probability to make the equation $e(X_u, P) = e(\tilde{Q}_u, PK_{anon})$ tenable.

Initialization: Assume challenger C provides system parameters $\{G_1, G_2, e, k, n, P, PK_{anon}, H_1, H_2, H_3\}$ for attacker F, and possesses (P, sP), in which $PK_{anon} = sP$, while s is the partial system key of TAS , and is unknown to C; the attacker F requests from C a random answer of Random Oracle Model H_1, and maintains consistency to avoid conflict, and C keeps a request-reply list to store the replies from the requests.

ROM query phase: C is able to provide ROM query for attacker F via ROM H_1, and provide corresponding request-reply parameters.

Attacker F conducts query via ROM H_1 to obtain harsh values, as follows:

H_1 request: F requests the hash value of identity ID_i from C, and C detects whether there is $ID_i \in L_I$ in request-reply list;

(1) If there is $ID_i \in L_I$, then send the corresponding reply to F.

(2) Otherwise, randomly selects $\tau_i \in Z_q^*$ and calculates $H_1(ID_i)$, send $(\tau_i, H_1(ID_i))$ to F, and stores this request-reply in the list L_I , then the corresponding $S_{ID_i} = \tau_i H_1(ID_i)$ can be easily obtained.

Forgeability and problem-solving: attacker F forges users registration information by masquerading TAS, but F is unable to obtain the partial system key s of TAS, and fails to calculate X_u , then the equation $e(X_u, P) = e(\tilde{Q}_u, PK_{anon})$ is invalid. If attacker F manages to obtain the random number $s \in Z_q^*$, then it has to guess random number s via the public key (P, PK_{anon}) and $PK_{anon} = sP$ in TAS, which means facing the calculative problem Diffie-Hellman, so attacker F is unable to solve Diffie-Hellman problem with non-negligible probability in polynomial time, which conflicts with the assumption. Therefore, the proposed scheme is able to meet the demand for non-forgeability.

5.3. **Query Tracing Attack.** Query tracing attack is also called continuous query attack, which means attacker could obtain user set in cloaking area at different time intervals according to continuous queries sent by one user, then speculate the user who requests the query by calculating the intersection of user sets in different cloaking areas. This scheme selects the optimal candidate to represent the initiator in requesting LBS, and the initiators role is played by the candidate in the whole course. So in the query records of LBS server, what is recorded is the ID information of the optimal candidate; meanwhile, at different time intervals in users mobility trajectories, there are different optimal candidates that represent real users in requesting LBS, so that attacker is unable to infer candidates relevancy to real users via the intersection of user sets in cloak area at different time intervals. Assume the frequency of users continuous query in mobility trajectories as k, and the number of candidates participating in each query is n_i, in which $1 \leq i \leq k$, since the optimal candidates in each query differ with one another, so the candidates in different cloak areas are independent with one another. Let $Pr(E)$ be the probability of attacker capturing and decrypting the communications between user U and candidate, then the probability of solving d_i based on PID_u is $Pr(ID)$. Suppose attacker obtains the registration request message from mobile terminal users to anonymous server, then in the course of continuous queries the probability of tracing users is $Pr = \prod_{i=1}^{k} \frac{1}{n_i} Pr(E) Pr(ID)$. $Pr(E)$ means solving the elliptic curve cryptosystem, which is infeasible in calculation. $Pr(ID)$ is equal to the known PID_u, then solve and find d_i according to equation $PID_u = D^T \bullet d_i$, while D is a n-dimensional column vector randomly selected by TAS, and the probability of solving and finding d_i is negligible; moreover, there are infinite solutions of the equation $Zd = p$, so attacker is unable to identify d_i according to matrix equations. Therefore, it can be concluded that the probability of attacker obtaining requestors real identity is negligible, that is, attacker is unable to trace candidates according to continuous query records so as to identify the real identity of the initiator.

6. **Simulation Experiment.** The environment of simulation experiment in this scheme is as follows: CPU: Intel i5 processor; RAM: 8G; operation system: Windows 7 (64 bit); simulation software: MATLAB; generator of mobile object: Thomas Brinkhoff. Suppose the experiment is conducted in an ideal network environment, then a large number of trajectory data of mobile objects are generated via Thomas Brinkhoff, and certain mobile object is selected randomly as the initiator to realize confusion of users trajectories by means of solution algorithm of similar trajectory in DTW and switch query algorithm, so as to further protect users trajectory privacy. In order to guarantee the authenticity of the experiment results, the following experiment results are invariably the average value of 1000 operations.

As is shown in Figure 2. given the fixed number of candidates, the processing time costs increase with increasing users and the point number N of trajectory segments. For example, when candidate K is 5, the point number N of trajectory segments increases from 2 to 10, while the processing time of the algorithm increases from 18ms to 41ms, which means the processing time is directly proportional to point number in trajectory segments. In the meantime, given the fixed point number of trajectory segments, the processing time increases with increasing candidates, for instance, when N =3, with the number of candidates being 5, 10 and 15 respectively, the processing time required is correspondently 21ms, 25ms and 31ms. The explanation is: when candidates for user or point number of trajectory segments increase, user needs to be matched with more candidates in certain domain, which would increase the operation time. Therefore, the total time costs in finding the optimal similar trajectories increase with increasing number of candidate users and number of point in trajectory segments. It is to be noted that two conditions must be met when this scheme is put into practice: $K \geq 2$ (K is the number of candidate users); $N \geq 2$ (N is the point number of trajectory). If the environment in which the request users lie is excessively sparse, for instance, when $K = 0$, no candidate exists to represent user in requesting service; when $K = 1$, that is, only one candidate exists, then it is the optimal candidate (without employing DTW algorithm) to replace user in requesting service, and attacker could trace it based on the candidates continuous queries. When $N = 1$ (N as the point number of trajectory segments), then this trajectory segment is replaced by this sampling point, which, obviously, means that the similarity of trajectory segments cannot be identified on the basis of a single point.

The results of the experiment shown in Figure. 3 reveal that among three schemes, the influence of candidate number K on the similarity of the selected optimal trajectories is invariably little. Given the same number of candidates K, Random scheme is the lowest in similarity, and the scheme in Reference [17] is relatively higher, while the scheme proposed in this paper proves to be the highest. The explanation: Random scheme doesnt take into account such elements as users behavioral patterns and trends, but only the false trajectories generated randomly; the scheme in Reference [17] takes into account those elements like users moving directions after each pause and accessibility when generating false trajectories, which improves the similarity of the generated false trajectories to users real trajectories; the proposed scheme adopts trajectory sampling and selects similar trajectories according to DTW algorithm, while short time intervals in sampling also shortens the candidate trajectories, so that the trajectory similarity is improved further than that of scheme [17].

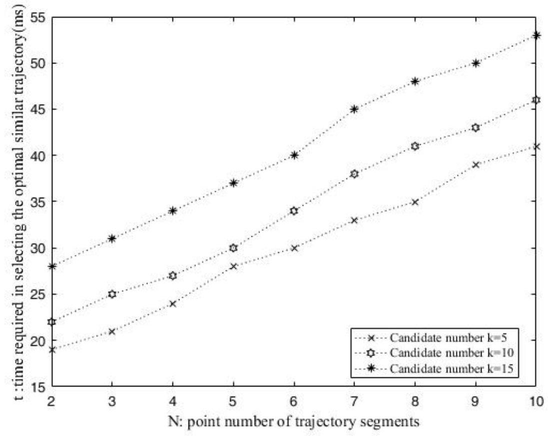

FIGURE 2. The influence of candidate number K and trajectory segments point number N on time t needed in selecting the optimal similar trajectory

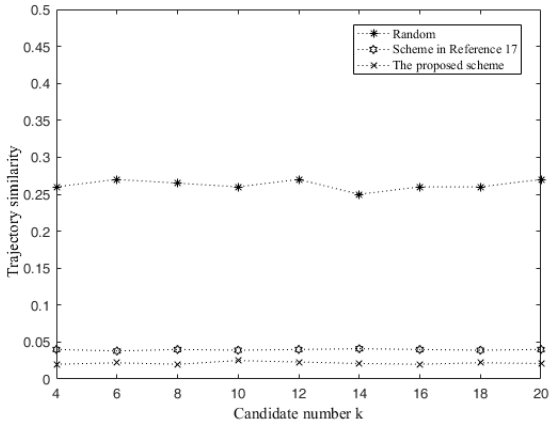

FIGURE 3. Comparison of the optimal trajectory similarity

7. **Summary.** Aiming at the problem that attacker may base its speculation on the data of users mobility trajectories so that users privacy information may take the risk of leaking, this paper proposes a trajectory privacy protection scheme based on DTW switch query. In this scheme, the identities of users requesting LBS service and of candidates are anonymized, then DTW algorithm is adopted to select the candidate with optimal trajectory similarity to represent real users in requesting LBS service, so that users identities and location privacy are protected. Security analyses prove that this scheme is not only able to solve such problems as anonymity and non-forgeability, but also able to resist the attack based on continuous queries. Simulation experiment is conducted to examine the candidate number K , point number N of trajectory segments and time t required by the algorithms, as well as the similarity in different schemes. The results show that the optimal candidate of the proposed scheme is better than that of other schemes in its similarity to real users at certain time intervals. Therefore, this scheme is of important theoretical significance and applicable value in mobile users privacy protection.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (61772159, 61300124, 61300216), the Science and Technology Research Program of He Nan Province (172102310677, 182102110333).

REFERENCES

[1] J. Krumm. A survey of computational location privacy, *Personal & Ubiquitous Computing*, vol. 13, no. 6, pp. 391-399, 2009.

[2] S. Tiwari, S. Kaushik, P. Jagwani, and S Tiwari. A Survey on LBS: System Architecture, Trends and Broad Research Areas, *Future Generation Computer Systems*, pp. 223-241, 2011.

[3] Y. M. Sun, M. Chen, L. Hug, Y. F. Qian, and M. M. Huang, ASA: Against statistical attacks for privacy-aware users in Location Based Service, *Future Generation Computer Systems*, vol. 70, 2016.

[4] Huo. Z, M. X. F. A Survey of Trajectory Privacy-Preserving Techniques, *Chinese Journal of Computers*, vol. 30, no. 10, pp. 1820-1830, 2011.

[5] D. Rebollo-Monedero, J. Forn, A. Solanas, and A. Martnez Ballest. Private location-based information retrieval through user collaboration, *Computer Communications*, vol. 33, no. 6, pp. 762-774, 2010.

[6] A. Khoshgozaran, C. Shahabi, H. Shirani-Mehr. Location privacy: going beyond K-anonymity, cloaking and anonymizers, *Springer-Verlag New York*, Inc. 2011.

[7] X. H. Li, M. x. Miao, H. Liu. J. F. Ma, and K. C. Li. An incentive mechanism for K -anonymity in LBS privacy protection based on credit mechanism, *Soft Computing*, vol. 21, no. 14, pp. 3907-3917, 2017.

[8] K. CK. Lee, B. Zheng, C. Chen, and C. Y. Chow. Efficient Index-Based Approaches for Skyline Queries in Location-Based Applications, *IEEE Transactions on Knowledge & Data Engineering*, vol. 25, no. 11, pp. 2507-2520, 2013.

[9] M. Gruteser, X. Liu. Protecting Privacy in Continuous Location-Tracking Applications, *IEEE Security & Privacy*, vol. 2, no. 2, pp. 28-34, 2004.

[10] Terrovitis M, Mamoulis N. Privacy Preservation in the Publication of Trajectories *International Conference on Mobile Data Management*, IEEE, pp. 65-72, 2008.

[11] R. Chen, B. CM. Fung, N. Mohammed, B. C. Desai, and K. Wang. Privacy-preserving trajectory data publishing by local suppression, *Information Sciences*, vol. 231, no. 1, pp. 83-97, 2013.

[12] J. Zhao, Y. Zhang. X. H. Li, and J. F. Ma. A Trajectory Privacy Protection Approach via Trajectory Frequency Suppression, *Chinese Journal of Computers*, vol. 37, no. 10, pp. 2097, 2014.

[13] P. R. Lei, W. C. Peng, I. J. Su, and C. P. Chang. Dummy-Based Schemes for Protecting Movement Trajectories, *Journal of Information Science & Engineering*, vol. 28, no. 2, pp. 335-350, 2012.

[14] J. Dai, L. Hua. A Method for the Trajectory Privacy Protection Based on the Segmented Fake Trajectory under Road Networks, *International Conference on Information Science and Control Engineering*, IEEE, pp. 13-17, 2015.

[15] C. Y. Chow, M. F. Mokbel. Enabling Private Continuous Queries for Revealed User Locations, *Advances in Spatial and Temporal Databases, International Symposium*,SSTD 2007, Boston, Ma, Usa, July 16-18, 2007, Proceedings. DBLP, pp. 258-275, 2007.

[16] Z. Huo, Y. Huang, X. Meng. History trajectory privacy-preserving through graph partition, *in Proc. ACM 1st Int. Workshop on Mobile Location-Based Service*, pp. 71-78, 2011.

[17] R. Kato, M. Iwata, T. Hara, A. Suzuki, and X. Xie. A dummy-based anonymization method based on user trajectory with pauses, *International Conference on Advances in Geographic Information Systems*, pp. 249-258, 2012.

[18] R. H. Hwang, Y. L. Hsueh, H. W. Chung. A Novel Time-Obfuscated Algorithm for Trajectory Privacy Protection, *IEEE Transactions on Services Computing*, vol. 7, no. 2, pp. 126-139, 2014.

[19] R. Schlegel, C. Y. Chow, Q. Huang, and D. S. Wong. User-Defined Privacy Grid System for Continuous Location-Based Services, *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2158-2172, 2015.

[20] T. Lam, K. Rietsch. Total positivity, Schubert positivity, and geometric Satake, *Journal of Algebra*, vol. 460, pp. 284-319, 2016.