Hindawi
Security and Communication Networks
Volume 2019, Article ID 2414687, 14 pages
https://doi.org/10.1155/2019/2414687

Research Article

A New Group Location Privacy-Preserving Method Based on Distributed Architecture in LBS

JingJing Wang,[1,2] **YiLiang Han**,[1,2] **XiaoYuan Yang**,[1,2,3] **TanPing Zhou**,[1,2,3] **and JiaYong Chen**[1]

[1] *College of Cryptography Engineering, Engineering University of People's Armed Police, Xi'an 710086, China*
[2] *Key Laboratory of Network & Information Security under the People's Armed Police, Xi'an 710086, China*
[3] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

Correspondence should be addressed to JingJing Wang; 344505421@qq.com and YiLiang Han; hanyil@163.com

Received 21 August 2018; Revised 4 January 2019; Accepted 20 January 2019; Published 14 February 2019

Academic Editor: Kuo-Hui Yeh

Nowadays, the location privacy problem has become an important problem for the users who enjoy the location-based services (LBSs). Researchers have focused on the problem of how to protect the location privacy of user efficiently for a long time. On one hand, many achievements adopt the centralized structure in which there is an additional center server. Additionally, some other researchers adopt the distributed structure to overcome the disadvantages brought by the center server in the centralized anonymous system structure. On the other hand, the existing methods of solving the problem are always to protect the individual user's location privacy in LBSs, without considering the user group's location privacy. This kind of methods is not very applicable to the status of a number of users who formed a group to complete a LBS task together by collaborative computing. In order to solve the problem of location privacy protection for a user group in the untrusted mobile social networks, a location privacy protection method based on the distributed structure is discussed in this paper. In the scheme, the special homomorphic features of BGN cryptosystem are cleverly used so that it can solve the group's three classical location service applications simultaneously, namely, group nearest neighbor query, optimal group collection point determination, and group friend's distance query, by only one security policy. If there are k users who formed the group, it could achieve k-anonymity without exposing the coordinate of each individual user or using any anonymous areas. Furthermore, theoretical and experimental analysis proves that the proposal can efficiently protect each user's location privacy in the group through taking full advantage of the collaborative computing and communication capabilities of the mobile terminals. It can resist the existing distance interaction attack and collusion attack and can realize the secure and efficient fine-grained controllable location privacy protection for the user group.

1. Introduction

LBSs experience a booming period of development due to the wide applications of location-based technology and the mobile terminals [1]. However, in the mobile social network, LBSs are usually provided by a server, which is called the location service provider (SP). Generally, in order to obtain good quality of LBSs, the users need to obey the policy set by the SP, that is, "informed consent," and have to provide their sensitive location information to the SP. However, most of the SPs are profit-oriented and they are not so reliable and trustworthy [2]. As a result, the users' real location information, even the related personal sensitive information such as living habits, interests, and health status, may be in danger of leaking and inferring. As an alternative, the users' location information might be completely hidden from the SP. In this scenario, the SP cannot provide the services with good quality or meet the application requirements. Therefore, how to balance the location privacy and the service quality is a key issue in the applications of LBSs.

Fortunately, with the development of the mobile networks, researchers have found many methods that can realize the location privacy-preserving in the applications of LBSs. The existing methods mainly can be divided into two big categories. (1) One is mixing the user's real location with a

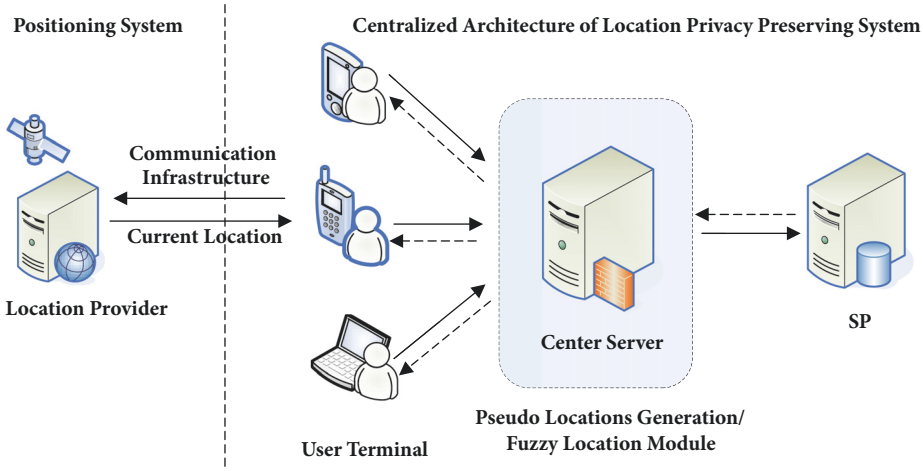

Figure 1: The location privacy-preserving system model with the centralized structure.

number of generalized fake locations. Then all the pseudolocations are sent to the SP together with the real location to get services. So it is difficult to tell which one is the user's real location. (2) The other is reducing the accuracy of user's location data. What the SP can get from the user is the fuzzy location information. Then the SP supports the service according to the fuzzy location.

No matter which kind of above methods is, it must be designed based on a certain system model. According to the perspective of system structure, there are two main types. They are, respectively, the centralized and distributed architecture. As shown in Figure 1, it is a location privacy-preserving model with the centralized system structure. The model is mainly composed of the user's mobile terminal, the trusted center server, and the SP. In this model, either the pseudolocations method or the fuzzy method can be used to protect the user's location privacy. Especially, in both methods, it is the trusted center server that completes the privacy protection work for the user's location and query information. Namely, the computation of pseudolocations or obfuscation of the real location is done by the center server. Examples can be found in [7–9], in which the centralized structure with the center server was employed. This kind of model is also the conventional design.

However, there are several shortcomings in the centralized location privacy-preserving model. (1) The center server must be trusted and dependable; otherwise the user's location collected by the server may face a serious threat. (2) Even if the center server is trustworthy, it still can become the performance bottleneck and the attack target in the applications. (3) The introduction of the center server brings the additional computation and communication consumptions. Moreover, it ignores the edge-computing capacity of the user's terminal.

In order to overcome the shortcomings of the centralized structure, more and more researches turn to the models with the distributed structure. For example, [10–14] all adopted the distributed architecture. The distributed structure system is only composed of the mobile terminals and SP. In this kind of structure, there is no central server. The users conduct the task of location privacy protection in LBSs together by their mobile terminals. In conclusion, various location privacy protection methods with different model structures have their own advantages. Researchers have considered various different scenarios and objects when designing their location privacy protection schemes.

Moreover, most of these existing schemes focus on the location privacy protection from the view of the individual user. They did not consider another frequent situation in practice. Sometimes, many users in the mobile networks are willing to form a group to collaborate when they issue the LBS. They want to realize their location privacy protection and obtain good service results with other users' cooperative computing. In the group, they can exchange some information but with their own location with other users of the same group for completing a task such as group nearest neighbor (GNN) query. Once the group jointly completes the query, each user in the group can adopt the query result returned in the LBS. However, the researches in this area are relatively rare and the existing schemes do not apply to the collaborative computing environment where many users complete the group query task together. Thus, it is necessary to design some schemes on the location privacy protection from the view of the user group.

2. Related Works

In fact, Hashem et al. [3] first researched on the user's location privacy problem in the GNN query. In their solution, each user's location in the group is fuzzied to its corresponding anonymous area. Then SP returns a series of candidate query results to the users in the group according to the anonymous areas. Then a filter algorithm is conducted to determine which one is nearest for all the users in the group. The solution has high communication overhead and cannot resist the collusion attack. In the same year, [15] proposed two schemes with centralized and distributed architecture, respectively, in the application of the GNN query. It adopts the multiparty

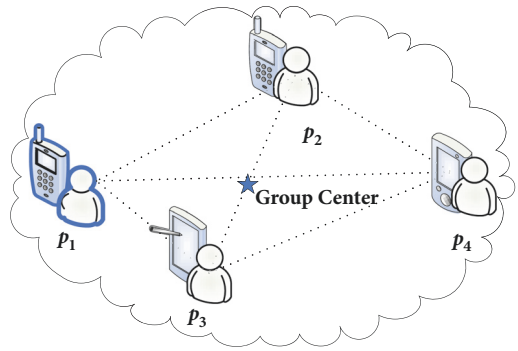

Figure 2: The center location of the user group.

computation to compute the object location so as to get the smallest sum of distances between the object location and all the users in the group. However, as its candidate target locations are predetermined, it would bring extra additional costs and overheads. Moreover, the leakage of distances threatened the user's location privacy in the group. Reference [6] proposed a group location privacy protection protocol (GLP), in which the Paillier cryptosystem [16] is used to compute the center location of the user group. However, because GLP needs to compute the AV-net [17] values in advance to realize protection, multiple different query messages and candidate response results will be generated in a single service. Moreover, each user in the group needs to broadcast his message. It occupies considerable resources and contributes to high communication cost. Indeed, back in 2008, [4] has already proposed a distributed location privacy protection scheme. It did not take the user group as the research object, but it used a number of users' disturbed location data to compute the centroid. Then it sent the centroid as the location to the SP for the nearest neighbor query in LBS. Actually, the intrinsice essence of the scheme is identical with [6]. Both [4, 6] turn the GNN query into nearest neighbor (NN) query of the group center so as to realize location privacy preserving. Similarly, [5] added random disturbance to the user's locations first. Then the disturbed locations are encrypted by Paillier cryptosystem to well protect each user's location privacy in the group. Furthermore, the group center location is figured out according to the secret sharing protocol. The scheme can well solve the privacy protection problem of the static GNN query. However, its construction is complex due to the secret sharing protocol. Its calculation overhead is high. The practicability is not strong.

At present, more and more researches about group privacy protection have focused on the key problem of the group center computation. It is proven that the group location privacy protection and the quality of LBS can be well balanced by changing the GNN query into NN query. Namely, as shown in Figure 2, in order to protect the location privacy of the user group, which is formed by users $p_2, \cdots, p_k$, the center location of the group is used as the geographic anchor point instead of the user's real location to issue queries. The SP gives the service results to the users in the group according to the center location. Therefore, the key problem of the group location privacy-preserving schemes is to calculate the center location without leaking each user's real location. Additionally, there is no doubt that the encryption technique can be used to protect the location privacy of the user group. But, until now, only a few works have been done in this area. And none of the outcomes mentioned above considered the quantitative measure or the controllability of the privacy protection effect from the view of the user.

In this paper, a new location privacy-preserving protocol for user group based on the distributed structure is designed. Each user's real location is added with a noise disturbance parameter to protect the user's location privacy. The weight coefficients are also introduced to ensure that the user who enjoys the LBS currently can freely adjust and control the contribution of other user's location data when computing the group center. Meanwhile, without exposing any user's real location coordinate, our scheme can realize only using one security policy, the core of BGN, to well solve three privacy protection problems in the classic LBS scenarios: the applications of GNN, the best group collection location determination, and the group friends distance query.

3. Our System Structure

3.1. Our System Model. Before the explanation of our scheme, this section puts forward our system model first. Shown as Figure 3, the distributed structure without any center server is adopted in our system model. Our system is mainly composed of the positioning system (such as global position system, BeiDou Navigation Satellite System, etc.), a user group, the communication networks, and the SP.

In order to simplify the problem, our system model assumes that if any user needs the LBS, he can easily form a group with nearby neighbors by the way of self-organized P2P network. In the group, users can communicate with each other and get their own location through the positioning system in real time. The privacy protection for each user is completed by the cooperation of the users in the group.

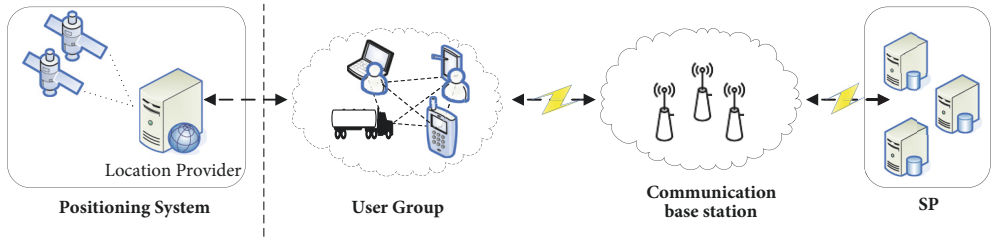

Figure 3: Our system model.

Compared with the existing models, in our model, the SP is semitrusted and the trusted center server is not necessary any more. It avoids the disadvantage brought by the request of trustworthy SP and the center server. The user who applies for LBS only sends the group center location as the anchor point instead of his own location to get good quality results from the SP. More importantly, our model ensures that each user never leaks their own real locations in the process of LBSs to any third party, including the other group users and the SP. Thus, it is more practical and effective in location privacy-preserving than other system models in the untrusted mobile networks.

3.2. Our System Basic Hypothesis. In view of the practical status of the mobile network, the system model is assumed as follows:

(1) The servers of the SP provide LBSs to the mobile users. Mobile users send LBS requests to the servers and receive corresponding location service results from the SP. In an open network environment, the SP will provide service results for users who request services. Moreover, in certain scenarios, the SP might analyze or disclose the user's real sensitive location information. Namely, the semitrusted SP is employed in this paper.

(2) The communication between mobile users and the SP is forwarded by the communication base station, and any third party can get and record the wireless messages transmitted by the base station.

(3) The mobile users obtain their real position coordinates from the position system or the location satellite anonymously.

(4) The mobile users have fine-granular demand for their location privacy and have the specific quality of service requirements.

(5) The users in the group distrust each other, and they will never expose or send their own real location to others.

3.3. Our System Symbols. For convenient describtion, Table 1 lists some symbols and parameters used in our system.

4. Our Method

4.1. Our Location Privacy-Protection Scheme of GNN Query

4.1.1. Initialization Definitions. When the user p_1 initiates the LBS at the time t, he will broadcast the message to the other neighbor users to invite them to form a group. If the user wants to form a group consisting of k members, he would confirm the first $k-1$ messages received from the other users. Thus, the $k-1$ users who responded to messages and obtained confirmations are selected to form the group together with p_1. In special case, if the number of user nodes is not enough, the broadcast range and hops should be increased, and the nodes that were accepted to form the group need to find more other nodes available for the group until k group users are accepted. Theoretically, if the group consists of k users, the scheme can realize k-anonymity for each user in the group. Because, in most cases, the $k-1$ users selected are the neighbor nodes around the user, the service results, such as GNN query result and best group collection location, are suitable for all the users in the group. In our method, we adopt the BGN cryptosystem as the security policy. BGN [18] is one of the most classical homomorphic cryptosystems. It can support homomorphic addition and one-time homomorphic multiplication simultaneously.

Definition 1. G_1, G_2 are additive groups, and G_T is a multiplicative group. The orders of G_1, G_2, G_T are all primes. $P \in G_1, Q \in G_2$ are the respective generators of G_1, G_2.

Bilinear mapping, $e : G_1 \times G_2 \longrightarrow G_T$, has the features as follows:

(1) Bilinearity:

$$\forall a, b \in \mathbb{Z}_p^*, e(P^a, Q^b) = e(P, Q)^{ab}.$$

(2) Nondegeneration: $e(P, Q) \neq 1$.

(3) With special condition, e can be computed effectively:

When $G_1 = G_2 = G_0$ and G_0 is a cyclic group, e has the feature of interchangeability:

$$\forall P, Q \in G_0, \quad e(P, Q) = e(Q, P). \tag{1}$$

Definition 2. Based on the bilinear mapping, the BGN cipher system is composed of three parts: key generation, encryption, and decryption.

Table 1: Symbol definitions.

$G = \{p_1, p_2, \cdots, p_k\}$	The group Gformed by the user nodes $p_1, p_2, \cdots, p_k$.
t	The certain time of the group user $p_1$ask for LBSs.
k	The group location privacy-preserving request.
$i = 1, 2, \cdots, k$	The subscript to mark symbols.
(x_i, y_i)	The geographic coordinate of the user p_i's location.
$\{w_i\}; \sum_{i=1}^{k} w_i = 1$	The weight sequence generated by the user p_1.
$(\alpha_i, \beta_i); \left(\frac{1}{k}\sum_{i=1}^{k}\alpha_i, \frac{1}{k}\sum_{i=1}^{k}\beta_i\right) = (0, 0)$	The noise sequence to disturb the users' location coordinate produced by the noise generator.
$\left(\hat{x}_i, \hat{y}_i\right) = (x_i + \alpha_i, y_i + \beta_i)$	The new coordinates after the disturbance by the noise.
$(X_G, Y_G) = (\sum_{i=1}^{k} w_i \hat{x}_i, \sum_{i=1}^{k} w_i \hat{y}_i)$	The center location of the user group G.

For key generation, each user in the system has a pair of keys distributed by the BGN cryptosystem, namely, the public key and the private key.

Set $\lambda \in \mathbb{Z}^+$ as a security parameter, and generate a tuple $(q_1, q_2, G_0, G_1{}', e)$, in which q_1, q_2 are two different large prime numbers. G_0 is a cyclic group of order q_1q_2; the bilinear mapping e is $G_0 \times G_0 \longrightarrow G_1{}'$. Set $N = q_1q_2$. Two generators g, u are chosen from G_0. Assuming that $h = u^{q_2}$, h is the generator with the order q_1 of the subgroup of G_0. $PK = \{N, G, G_1{}', e, g, h\}$, and $SK = q_1$. If the parameters are selected by the user p_1, then p_1's public key is PK and the private key is SK.

For encryption, suppose that the space of the plaintext messages is made up by the integers of the set $\{0, 1, \cdots, T\}$, where $T < q_2$. Using the public key PK to encrypt the message m, selecting a random number r, $r \in \{1, 2, \cdots, N\}$, then calculate:

$C = g^m h^r \in G_0$, where C is the ciphertext.

For decryption, use the private key $SK = q_1$ to decrypt the ciphertext:

$$C^{q_1} = \left(g^m h^r\right)^{q_1} = \left(g^m u^{rq_2}\right)^{q_1} = \left(g^{q_1}\right)^m, \quad m = \log_{g^{q_1}} C^{q_1}. \tag{2}$$

So the user p_1 can compute out m by his private key. Moreover, here $0 \le m \le T$; the time complexity of the solution would be $o(\sqrt{T})$ [19].

Definition 3. The BGN cryptosystem can support homomorphic addition and one-time homomorphic multiplication simultaneously.

Our method adopts the secure policy of BGN cryptosystem, and our solutions validity depends on its homomorphic property. Here, we prove the homomorphic property of BGN cryptosystem. For convenient explanation, the encryption algorithm of BGN cryptosystem is denoted by $E_*(\cdot)$, and its decryption algorithm is $D_*(\cdot)$.

(1) Additive Homomorphism. Set $E_{PK}(m_1) = C_1 = g^{m_1}h^{r_1} \in G_0$, $E_{PK}(m_2) = C_2 = g^{m_2}h^{r_2} \in G_0$ as the respective corresponding ciphertext of the plaintext $m_1, m_2 \in \{0, 1, \cdots, T\}$.

If $C = C_1C_2h^r$, then

$D_{SK}(C) = D_{SK}(C_1C_2h^r) = D_{SK}((g^{m_1}h^{r_1})(g^{m_2}h^{r_2})h^r) = D_{SK}(g^{m_1+m_2}h^{r_1+r_2+r}) = m_1 + m_2$ is established, where $r \in \{1, 2, \cdots, N-1\}$ is randomly chosen.

(2) One-Time Multiplicative Homomorphism. Set $g_1 = e(g, g), h_1 = e(g, h)$; and the order of g_1 is N and the order of h_1 is q_1. Moreover, there is $\mu \in \mathbb{Z}$, meeting $h = g^{\mu q_2}$ and $C = e(C_1, C_2){h_1}^r$. So the following equation is correct:

$$\begin{aligned} D_{SK}(C) &= D_{SK}\left(e\left(C_1, C_2\right){h_1}^r\right) \\ &= D_{SK}\left(e\left(g^{m_1}h^{r_1}, g^{m_2}h^{r_2}\right){h_1}^r\right) \\ &= D_{SK}\left(e\left(g^{m_1+\mu q_2 r_1}, g^{m_2+\mu q_2 r_2}\right){h_1}^r\right) \\ &= D_{SK}\left(e\left(g, g\right)^{(m_1+\mu q_2 r_1)(m_2+\mu q_2 r_2)}{h_1}^r\right) \\ &= D_{SK}\left(e\left(g, g\right)^{m_1m_2+\mu q_2(m_1r_2+m_2r_1+\mu r_1r_2q_2)}{h_1}^r\right) \\ &= D_{SK}\left(e\left(g, g\right)^{m_1m_2}{h_1}^{r+m_1r_2+m_2r_1+\mu r_1r_2q_2}\right) \\ &= m_1m_2 \mod N. \end{aligned} \tag{3}$$

Thus, the result of the operation on the plaintexts can be also got by decrypting the corresponding operation result of the ciphertexts [20]. For example, in our method, the group center can be obtained only depending on the computation of the ciphertexts from the users' real sensitive locations. It can be directly decrypted from the processed result of the encrypted users' locations. This theory will be elaborated in the next section.

4.1.2. Scenario Description. An important type of LBSs is the point of interest query, also known as location searching services (LSSs) [14]. User can find nearby interest point location and get corresponding distances to the desired

location through LSSs. Actually, LSSs include many classic applications of LBSs, such as finding nearby interest locations or friends and determining the optimal collection location. In this section, the scheme is designed in the scenario of GNN query. For the premise of location privacy-preserving, the users in the group need to cooperate with one another to complete the query task without exposing their real location information.

4.1.3. Scheme Description. Here, we assume that the user p_1 first wants to apply for the GNN query, and he has already formed the group with other $k-1$ users $p_2, \cdots, p_k$. Additionally, the digital signature of the user p_i is denoted as $Sig_i(\cdot)$.

(1) p_1 sends the message $\{(E_{PK}(\hat{x_1}), E_{PK}(\hat{y_1})), \{w_i\}, t, Sig_1\}$ to the SP, and $p_2, \cdots, p_k$, respectively, send the message $\{(E_{PK}(\hat{x_i}), E_{PK}(\hat{y_i})), t, Sig_i\}$ to the SP, where $(i = 2, \cdots, k)$.

(2) After receiving the above messages, SP executes the computation as (4a) to obtain the functions of U_1, U_2; then the results of the functions are sent to the user p_1:

$$\begin{aligned} U_1 &= \left(E\left(\hat{x_1}\right)^{w_1} \times E\left(\hat{x_2}\right)^{w_2} \times \cdots \times E\left(\hat{x_k}\right)^{w_k}\right) h^r; \\ U_2 &= \left(E\left(\hat{y_1}\right)^{w_1} \times E\left(\hat{y_2}\right)^{w_2} \times \cdots \times E\left(\hat{y_k}\right)^{w_k}\right) h^{r'}. \end{aligned} \tag{4a}$$

(3) U_1, U_2 are received by p_1, p_1 to decrypt them as (4b) to calculate (X_G, Y_G), which is the center location of the group at the time t:

$$\begin{aligned} X_G &= D_{SK}(U_1) = \sum_{i=1}^{k} w_i \left(\hat{x_i}\right); \\ Y_G &= D_{SK}(U_2) = \sum_{i=1}^{k} w_i \left(\hat{y_i}\right). \end{aligned} \tag{4b}$$

(4) (X_G, Y_G) is used as the anchor point to be sent to the SP by p_1 for obtaining the query service. Meanwhile, the message (X_G, Y_G, t, sig_1) is broadcasted to all the other group user nodes $p_2, p_3, \cdots, p_k$.

(5) The SP sends the result to p_1 according to the anchor point received. In addition, when the other group users need to issue similar location queries, they also assume (X_G, Y_G) as the anchor point and send the requests to the SP to obtain the corresponding services.

4.2. Our Location Privacy-Protection Scheme of the Group Best Collection Location Query

4.2.1. Scenario Description. Sometimes, there is an important application in LBSs. It is the query for the group collection location. The friends may want to determine some location to gather around. In this case, they can form a temporary group to obtain the optimal collection location. For the users in the group, finding the optimal location is finding the location that meets the sum of distances to everyone in the group is smallest. Moreover, in order to ensure the group privacy, the best collection location should be safely determined without exposing any user's real location.

Definition 4. If the sum of the distances from some location point to all the group users is minimum, the point is the best assembling location of the user group, which is expressed as O. It means to calculate the coordinate value (x_o, y_o) of O, which satisfies the following equation: $d_{\min} = \min(\sum_{i=1}^{k}((x_o - x_i)^2 + (y_o - y_i)^2))$.

4.2.2. Scheme Description. Assume that the user p_1 applies for the group best collection location query services:

(1) $p_1, p_2, \cdots, p_k$, respectively, send the messages $\{(E_{PK}(\hat{x_i}), E_{PK}(\hat{y_i})), t, Sig_i\}$ to SP, where $(i = 2, \cdots, k)$.

(2) The SP calculates U_{o1}, U_{o2} according to (4c) after receiving the above messages and then sends them to the user p_1:

$$\begin{aligned} U_{o1} &= \left(E_{PK}\left(\hat{x_1}\right) \times E_{PK}\left(\hat{x_2}\right) \times \cdots \times E_{PK}\left(\hat{x_k}\right)\right) h^r \\ U_{o2} &= \left(E_{PK}\left(\hat{y_1}\right) \times E_{PK}\left(\hat{y_2}\right) \times \cdots \times E_{PK}\left(\hat{y_k}\right)\right) h^{r'}. \end{aligned} \tag{4c}$$

(3) The user p_1 computes the values of c_1, c_2 and the coordinate value (x_o, y_o) of the location point O according to (4d):

$$\begin{aligned} D_{SK}(U_{o1}) &= x_1 + x_2 + \cdots + x_k = \sum_{i=1}^{k}(x_i) = c_1 \\ D_{SK}(U_{o2}) &= y_1 + y_2 + \cdots + y_k = \sum_{i=1}^{k}(x_i) = c_2 \end{aligned} \tag{4d}$$

where $(x_o = c_1/k, y_o = c_2/k)$.

4.3. Our Privacy-Protection Scheme of Group Friends Distance Query

4.3.1. Scenario Description. Sometimes, in LBSs, users want to know their friend's distance from them. In this case, from the view of location privacy protection, we should ensure that each user in the group could conveniently inquire the friend's distance without exposing his own location information or knowing his friend's location. This case is similar to another application in LBSs that the merchants or shops would like to push advertisements to the users based on their locations. The merchants and shops concerned by the group users can safely inquire the distance from the user and decide whether to push advertisements to some user in the group without knowing the specific location of the users.

4.3.2. Scheme Description. Assume that the group user p_1 applies for the friend's distance query services:

(1) The user p_1 sends the friend distance query service request to the SP so as to query the friend p_i's distance.

(2) After receiving the query request, the SP calculates the function of the ciphertexts U_{dis} according to (4e) and sends U_{dis} to the user p_1:

$$U_{dis} = \begin{pmatrix} e\left(\left(E_{PK}\left(x_1+\alpha\right)E_{PK}\left(-x_i-\alpha\right)h^r\right), \left(E_{PK}\left(x_1+\alpha\right)E_{PK}\left(-x_i-\alpha\right)h^r\right)\right){h_1}^{r'} \\ \times e\left(\left(E_{PK}\left(y_1+\beta\right)E_{PK}\left(-y_i-\beta\right)h^r\right), \left(E_{PK}\left(y_1+\beta\right)E_{PK}\left(-y_i-\beta\right)h^r\right)\right){h_1}^{r'} \end{pmatrix} h^{r_3}. \tag{4e}$$

(3) p_1 receives the value of U_{dis} and decrypts it so as to obtain the distance between p_1 and p_i according to (4f):

$$D_{SK}\left(U_{dis}\right) = \left(\left(x_1-x_i\right)^2 + \left(y_1-y_i\right)^2\right) \mod N. \tag{4f}$$

5. Safety and Performance Analysis

5.1. Validity Analysis

Theorem 5. *In the scheme proposed in Section 4.1 of this paper, the group users can convert the group POI location query to the query of the corresponding centroid of the group.*

Proof. Based on the homomorphism property of BGN cryptosystem, the correctness of our method to get the center location can be further proven:

$$\begin{aligned} &D_{SK}\left(\left(E_{PK}\left(\hat{x_1}\right)^{w_1} \times E_{PK}\left(\hat{x_2}\right)^{w_2} \times \cdots \times E_{PK}\left(\hat{x_k}\right)^{w_k}\right)h^r\right) = D_{SK}\left(\left(E_{PK}\left(x_1+\alpha_1\right)^{w_1} \times E_{PK}\left(x_2+\alpha_2\right)^{w_2} \times \cdots \times E_{PK}\left(x_k\right.\right.\right. \\ &\left.\left.\left.+\alpha_k\right)^{w_k}\right)h^r\right) = D_{SK}\left(\left(\left(g^{x_1}g^{\alpha_1}h^{r_1}\right)^{w_1} \times \left(g^{x_2}g^{\alpha_2}h^{r_2}\right)^{w_2} \times \cdots \times \left(g^{x_k}g^{\alpha_k}h^{r_k}\right)^{w_k}\right) \times h^r\right) = D_{SK}\left(\left(g^{x_1w_1}g^{w_1\alpha_1}h^{r_1w_1}\right)\right. \\ &\left.\times \left(g^{x_2w_2}g^{w_2\alpha_2}h^{r_2w_2}\right) \times \cdots \times \left(g^{x_kw_k}g^{w_k\alpha_k}h^{r_kw_k}\right) \times h^r\right) = D_{SK}\left(\left(g^{x_1w_1+x_2w_2+\cdots+x_kw_k+w_1\alpha_1+w_2\alpha_2+\cdots+w_k\alpha_k}\right)\right. \\ &\left.\cdot h^{r_1w_1+r_2w_2+\cdots+r_kw_k+r_1w_1+r_2w_2+\cdots+r_kw_k}h^r\right) = D_{SK}\left(\left(g^{x_1w_1+x_2w_2+\cdots+x_kw_k+w_1\alpha_1+w_2\alpha_2+\cdots+w_k\alpha_k}h^{r_1w_1+r_2w_2+\cdots+r_kw_k+r_1w_1+r_2w_2+\cdots+r_kw_k+r}\right)\right) \\ &= x_1w_1 + x_2w_2 + \cdots + x_kw_k + w_1\alpha_1 + w_2\alpha_2 + \cdots + w_k\alpha_k = \sum_{i=1}^{k} w_i\left(\hat{x_i}\right) = X_G. \end{aligned} \tag{5}$$

Similarly, we can prove:

$$D_{SK}\left(\left(E_{PK}\left(\hat{y_1}\right)^{w_1} \times E_{PK}\left(\hat{y_2}\right)^{w_2} \times \cdots \times E_{PK}\left(\hat{y_k}\right)^{w_k}\right) \cdot h^r\right) = \sum_{i=1}^{k} w_i\left(\hat{y_i}\right) = Y_G. \tag{6}$$

□

In addition, according to the analysis and conclusion in [5], it can be further proven that the scheme in Section 4.1 is valid. The centroid coordinate (X_G, Y_G) of the user group can be obtained so as to achieve POI query of the group centroid and obtain the applicable LBS results.

Theorem 6. *In the scheme proposed in Section 4.2 of this paper, the group users can obtain the best collection location coordinates.*

Proof. First, we can calculate the best collection location by solving mathematical minimization problem. Compute the value of coordinate of point $O(x_o, y_o)$ which satisfies the condition $d_{\min} = \min(\sum_{i=1}^{k}((x_o - x_i)^2 + (y_o - y_i)^2))$.

Solve the following problem:

$$\begin{aligned} d_{\min} &= \min\begin{pmatrix} k\left({x_o}^2 + {y_o}^2\right) - 2x_o\left(x_1 + x_2 + \cdots + x_k\right) - 2y_o\left(y_1 + y_2 + \cdots + y_k\right) \\ + \left({x_1}^2 + {x_2}^2 + \cdots + {x_k}^2\right) + \left({y_1}^2 + {y_2}^2 + \cdots + {y_k}^2\right) \end{pmatrix} \\ &= \min\left(k\left({x_o}^2 + {y_o}^2\right) - 2x_oc_1 - 2y_oc_2 + c_3\right). \end{aligned} \tag{7}$$

Here, k, c_1, c_2, c_3 are all constants:

$$c_1 = \sum_{i=1}^{k} x_i;$$
$$c_2 = \sum_{i=1}^{k} y_i; \quad (8)$$
$$c_3 = \sum_{i=1}^{k} \left(x_i^2 + y_i^2\right).$$

Set $Z = (k(x_o^2 + y_o^2) - 2x_o c_1 - 2y_o c_2 + c_3)$, and take the partial derivative of Z:

$$\frac{\partial Z}{\partial x_o} = 2kx_o - 2c_1;$$
$$\frac{\partial Z}{\partial y_o} = 2ky_o - 2c_2;$$
$$\frac{\partial^2 Z}{\partial x_o^2} = 2k > 0 \quad (9)$$
$$\frac{\partial^2 Z}{\partial y_o^2} = 2k > 0$$

Therefore the minimum value of $Z = (k(x_o^2 + y_o^2) - 2x_o c_1 - 2y_o c_2 + c_3)$ is obtained at the point $(x_o = c_1/k, y_o = c_2/k)$, which is also the best gathering location for the group G.

Furthermore, we can prove the equation as follows by the homomorphism property of BGN cryptosystem:

$$\begin{aligned} &D_{SK}\left(\left(E_{PK}\left(\hat{x_1}\right) \times E_{PK}\left(\hat{x_2}\right) \times \cdots \times E_{PK}\left(\hat{x_k}\right)\right) h^r\right) \\ &= D_{SK}\left(\left(E_{PK}(x_1 + \alpha_1) \times E_{PK}(x_2 + \alpha_2) \times \cdots\right.\right. \\ &\left.\left. \times E_{PK}(x_k + \alpha_k)\right) h^r\right) = D_{SK}\left(\left(g^{x_1} g^{\alpha_1} h^{r_1}\right)\right. \\ &\left. \times \left(g^{x_2} g^{\alpha_2} h^{r_2}\right) \times \cdots \times \left(g^{x_k} g^{\alpha_k} h^{r_k}\right) \times h^r\right) \\ &= D_{SK}\left(\left(g^{x_1 + x_2 + \cdots + x_k + \alpha_1 + \alpha_2 + \cdots + \alpha_k}\right)\right. \\ &\left. \cdot h^{r_1 + r_2 + \cdots + r_k + r_1 + r_2 + \cdots + r_k} h^r\right) \\ &= D_{SK}\left(\left(g^{x_1 + x_2 + \cdots + x_k} h^{r_1 + r_2 + \cdots + r_k + r_1 + r_2 + \cdots + r_k + r}\right)\right) = x_1 \\ &+ x_2 + \cdots + x_k = \sum_{i=1}^{k} (x_i) = c_1 \end{aligned} \quad (10)$$

and

$$\begin{aligned} &D_{SK}\left(\left(E_{PK}\left(\hat{y_1}\right) \times E_{PK}\left(\hat{y_2}\right) \times \cdots \times E_{PK}\left(\hat{y_k}\right)\right) h^{r'}\right) \\ &= D_{SK}\left(\left(E_{PK}(y_1 + \beta_1) \times E_{PK}(x_2 + \beta_2) \times \cdots\right.\right. \\ &\left.\left. \times E_{PK}(x_k + \beta_k)\right) h^{r'}\right) = c_2. \end{aligned} \quad (11)$$

Additionally, we must notice that the best collection location point here is decided by the minimum sum of distances. In reality, we should also consider that the time interval between the first user with the shortest distance d_{oi} and the last user with the longest distance d_{oj} is too long beyond the group users' tolerance levels. Assuming that the acceptable max time interval is Δt, and when under the condition of the same velocity $v_i = v_j = v$, it is equal to solve the minimum value problem with an added constraint: $|(d_{oi} - d_{oj})/v| \leq \Delta t$. Moreover, if the users' velocities are different, the added constraint is $|d_{oi}/v_i - d_{oj}/v_j| \leq \Delta t$. □

Theorem 7. *In the scheme proposed in Section 4.3 of this paper, the group users can obtain the friend's distance value.*

Proof.

$$\begin{aligned} &D_{SK}\left(\begin{pmatrix} e\left(\left(E_{PK}(x_1 + \alpha) E_{PK}(-x_i - \alpha) h^r\right), \left(E_{PK}(x_1 + \alpha) E_{PK}(-x_i - \alpha) h^r\right)\right) {h_1}^{r'} \\ \times e\left(\left(E_{PK}(y_1 + \beta) E_{PK}(-y_i - \beta) h^r\right), \left(E_{PK}(y_1 + \beta) E_{PK}(-y_i - \beta) h^r\right)\right) {h_1}^{r'} \end{pmatrix} {h_2}^{r_3}\right) \\ &= D_{SK}\left(\begin{pmatrix} e\left(\left(g^{x_1} g^{\alpha} h^{r_1} g^{-x_i} g^{-\alpha} h^{r_2} h^r\right), \left(g^{x_1} g^{\alpha} h^{r_1} g^{-x_i} g^{-\alpha} h^{r_2} h^r\right)\right) {h_1}^{r'} \\ \times e\left(\left(g^{y_1} g^{\beta} h^{r_1'} g^{-y_i} g^{-\beta} h^{r_2'} h^r\right), \left(g^{y_1} g^{\beta} h^{r_1'} g^{-y_i} g^{-\beta} h^{r_2'} h^r\right)\right) {h_1}^{r'} \end{pmatrix} {h_2}^{r_3}\right) \\ &= D_{SK}\left(\left(e\left(g^{x_1 - x_i} h^{r_1 + r_2 + r}, g^{x_1 - x_i} h^{r_1 + r_2 + r}\right) {h_1}^{r'} \times e\left(g^{y_1 - y_i} h^{r_1' + r_2' + r}, g^{y_1 - y_i} h^{r_1' + r_2' + r}\right) {h_1}^{r'}\right) {h_2}^{r_3}\right) \\ &= D_{SK}\left(\left(e\left(g^{x_1 - x_i + \mu q_2 (r_1 + r_2 + r)}, g^{x_1 - x_i + \mu q_2 (r_1 + r_2 + r)}\right) {h_1}^{r'} \times e\left(g^{y_1 - y_i + \mu q_2 (r_1' + r_2' + r)}, g^{y_1 - y_i + + \mu q_2 (r_1' + r_2' + r)}\right) {h_1}^{r'}\right) {h_2}^{r_3}\right) \\ &= D_{SK}\left(\left(e(g, g)^{(x_1 - x_i + \mu q_2 (r_1 + r_2 + r))(x_1 - x_i + \mu q_2 (r_1 + r_2 + r))} {h_1}^{r'} \times e(g, g)^{(y_1 - y_i + \mu q_2 (r_1' + r_2' + r))(y_1 - y_i + \mu q_2 (r_1' + r_2' + r))} {h_1}^{r'}\right) {h_2}^{r_3}\right) \end{aligned}$$

$$= D_{SK}\left(\begin{pmatrix} e(g,g)^{(x_1-x_i)(x_1-x_i)}\, h_1{}^{r'+\mu q_2((r_1+r_2+r)(r_1+r_2+r)+x_1(r_1+r_2+r)-x_i(r_1+r_2+r))} \\ \times e(g,g)^{(y_1-y_i)(y_1-y_i)}\, h_1{}^{r'+\mu q_2((r_1{}'+r_2{}'+r)(r_1{}'+r_2{}'+r)+y_1(r_1{}'+r_2{}'+r)-y_i(r_1{}'+r_2{}'+r))} \end{pmatrix} h_2{}^{r_3}\right)$$

$$= \left((x_1-x_i)(x_1-x_i)+(y_1-y_i)(y_1-y_i)\right) \mod N = \left((x_1-x_i)^2+(y_1-y_i)^2\right) \mod N \tag{12}$$

where $h \in G_0, h_1 \in G_1$.

Therefore, Theorem 7 is proven. □

5.2. Privacy Security Analysis

5.2.1. The Quantitative Measurements of the Privacy Security and the Quality of LBSs. In this section, some quantitative measurements of privacy security and quality of services are given according to our method. In our privacy model, the quantitative measurements can be obtained easily by the relationships between the group center location and each user's real location.

(1) The geometric measures of the group location privacy-preserving

(a) The location privacy protection distance: it is the Euclidean distance between the user p_i and the determined centroid, which is defined as

$$Dis_{LP_i}{}^2 = (X_G - x_i)^2 + (Y_G - y_i)^2. \tag{13}$$

(b) The maximum distance of the group privacy protection: assuming that the maximum distance is obtained between the group user p_i and the center location, it can be defined as

$$Dis_{LP\max}{}^2 = \max\left((X_G - x_i)^2 + (Y_G - y_i)^2\right). \tag{14}$$

(c) The minimum distance of the group privacy protection: assuming that the minimum distance is obtained between the group user p_i and the centroid, it can be defined as

$$Dis_{LP\min}{}^2 = \min\left((X_G - x_i)^2 + (Y_G - y_i)^2\right). \tag{15}$$

(d) The location privacy protection angle: it refers to the declination angle between the user p_i and the group center, which is defined as

$$\theta_{LP_i} = \arctan\frac{|Y_G - y_i|}{|X_G - x_i|}; \quad (Y_G \neq y_i, X_G \neq x_i). \tag{16}$$

Thus, the measurements proposed are very suitable for our privacy model. It is possible for the user to easily judge and control the privacy protection degree by the measurements.

Theorem 8. *The users in the group can adjust the weight sequence $\{w_1, w_2, \cdots, w_k\}$ to adjust the values of Dis_{LP_i} and θ_{LP_i} so as to freely control the degree of the location privacy-protection according to their own privacy request.*

Proof. From the perspective of LBSs, the user gets the query results according to his own position. In our method, all the users in the group get the query results from the SP according to the group center instead of their own positions. Especially, because the users in the group have different geographic locations, the distance of the group center location to different users in the group may be different, which can be seen in Figure 4. $p_1, \cdots, p_4$ are the users who formed the group to get LBSs. Their geolocation coordinates are $(x_1, y_1), \cdots, (x_4, y_4)$. They can calculate the group center $o(x_G, y_G)$ and send o to the SP to get query results. Therefore, they can get the good quality of services without exposing their own locations. However, in this case, there is a distance from each user to the group center. The distance is changeable according to the value of Dis_{LP_i}. For instance, in the GNN query, because the query is converted to the NN query, the group center is the anchor point to the SP. Thus, with the increase of Dis_{LP_i}, the effect of location privacy-protection for the user p_i improves. Conversely, because the group center is farther away from p_i, the quality of the GNN query service might be worse. Furthermore, in Figure 4, if $Dis_{LP_1} > Dis_{LP_2}$, the effect of location privacy protection for $p_1$is better than the effect for p_2. □

Because $(X_G, Y_G) = (\sum_{j=1}^{k} w_j \hat{x}_j, \sum_{i=1}^{k} w_j \hat{y}_j)$, we can get the equation as follows:

$$\begin{aligned} Dis_{LP_i}{}^2 &= (X_G - x_i)^2 + (Y_G - y_i)^2 \\ &= \left(\left(\sum_{j=1}^{k} w_j \hat{x}_j\right) - x_i\right)^2 \\ &\quad + \left(\left(\sum_{j=1}^{k} w_j \hat{y}_j\right) - y_i\right)^2. \end{aligned} \tag{17}$$

From the above equation, since (x_i, y_i) is not changeable in a query, the value of Dis_{LP_i} mainly depends on the group center (X_G, Y_G). (X_G, Y_G) relies on the weight coefficients and the noise parameters assigned to each user in the group by p_i. Generally, the noise sequence is fixed. Ultimately, Dis_{LP_i} is determined by the weight coefficients $\{w_1, w_2, \cdots, w_k\}$. p_i can increase or decrease Dis_{LP_i} by adjusting the weight coefficients assigned to different users in the group in order to get better service quality or better location privacy in LBSs. Meanwhile, by adjusting the values of $\{w_1, w_2, \cdots, w_k\}$, p_i can weaken or strengthen the contribution brought by each user's location to the computation of group center according to the

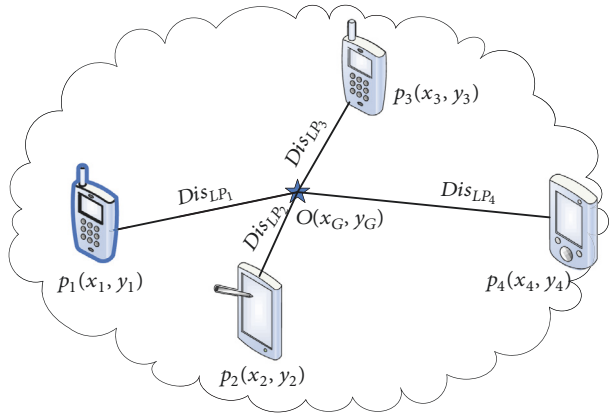

Figure 4: The geometric measures of the group location privacy protection.

characteristics of the users, such as their reliability, online time, intimacy relationship, and the distance.

Usually, each user in the group has different requirements for location privacy-protection. The user who has the highest request for location privacy-preserving always should have the largest privacy-protection distance $Dis_{LP\max}$. However, the user who has the higher request for the quality of services always has smaller privacy-protection distance $Dis_{LP\min}$ in order to ensure that the query location of NN is closest to himself. Therefore, users in the group can measure and control the degree of privacy protection and quality of services.

Similarly, from the definition of θ_{LP_i}, we can also get the following equation:

$$\theta_{LP_i} = \arctan \frac{|Y_G - y_i|}{|X_G - x_i|} = \arctan \frac{\left|\left(\sum_{j=1}^{k} w_j \hat{y}_j\right) - y_i\right|}{\left|\left(\sum_{j=1}^{k} w_j \hat{x}_j\right) - x_i\right|}. \quad (18)$$

θ_{LP_i} stands for the protecting extent of the separate longitude and latitude of p_i. The value of θ_{LP_i} can be decided by $\{w_1, w_2, \cdots, w_k\}$ too. Especially, if $(X_G \neq x_i; Y_G = y_i)$, it only realizes the obscuration of the longitude of p_i's real location coordinate. If $(X_G = x_i; Y_G \neq y_i)$, the protection only realizes the obscuration of the latitude of p_i's location. Additionally, if $(Y_G = y_i; X_G = x_i)$, the degree of the protection for p_i is nearly zero, but the quality of LBSs, such as GNN query, is best. Therefore, p_i can also change the values of $\{w_1, w_2, \cdots, w_k\}$ for adjusting the value of θ_{LP_i}. Compared with Dis_{LP_i}, θ_{LP_i} makes it possible for p_i to measure and control the effect of location privacy-protection from a smaller granularity.

(2) The geometric measures of the GNN service

As shown in Figure 5, assume that the service result of the current GNN query returned to the group is the point S. Its angle with o is denoted as θ_{OP}. The Euclidean distance between S and p_i is denoted as D_i, and the Euclidean distance between S and O is Dis_{OP}. Then the geometric measure of the quality of the user p_i's NN query service in the group can be defined as the actual distance between the user p_i and S.

In order to simplify the problem description and facilitate quantitative measurement, the Euclidean distance D_i is used to stand for the actual distance between S and p_i in the geographical map. So we can have

$$D_i^2 = Dis_{LP}^2 + Dis_{OP}^2 + 2Dis_{LP} \times Dis_{OP} \cos\left(\theta_{OP} - \theta_{LP}\right). \quad (19)$$

What is more, from the perspective of a single user in the group, when the NN query result is S, the actual traffic distance on the map between the user p_i and S can directly measure the quality of the current service obtained by p_i. Obviously, from the view of the single user p_i, the smaller D_i is, the better the quality of NN query service is. However, from the perspective of the whole group, it is necessary to consider the overall quality of services after forming the group. Therefore, calculating the total distances from S to all the users in the group is reasonable. The smaller $\sum_{i=1}^{k} D_i$ is, the better the quality of current GNN query services is.

5.2.2. Privacy Security Analysis. In fact, in LBSs, exposing precise user positions raises user privacy concerns, especially if the SP is not fully trusted. To enable the secure applications of private user locations in nontrusted networks, we present three kinds of group location privacy protection schemes in three important application scenarios. In our method, there is no need to provide individual location data of each user to the SP. Only the aggregation result of the group users' locations is usually required to obtain the corresponding query results [21]. In our schemes, the aggregation results are different aggregated computations of the ciphertexts from the users' locations in the group.

Theorem 9. *The schemes in Sections 4.1, 4.2, and 4.3 in this paper can realize the group location privacy-protection, as*

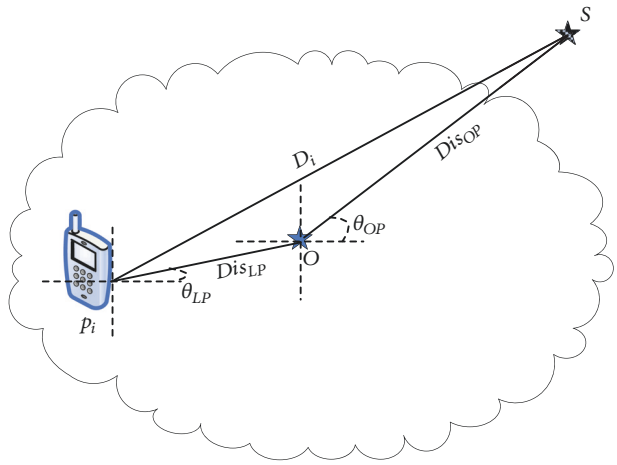

Figure 5: The geometric measures of the quality of GNN query service.

well as each user's location privacy-protection in the group. Moreover, they can resist the collusion attack and the dynamic distance interaction attack.

Proof. (1) In the scheme of Section 4.1, the group users $p_2, \cdots, p_k$ encrypt their real location coordinates after noise perturbation and weights adding by using the public key of the user p_1 who has applied for the LBSs. Because the users are independent of one another, the encryption of each user's location can be calculated in parallel. Then the SP completes the intermediate outsourced calculation of the ciphertexts encrypted by the users in the group and sends the aggregated result of the ciphertexts back to p_1. At last, p_1 decrypts the result by using his own private key to obtain the group center and corresponding query service response from the SP.

In the process of LBSs, the users' locations are encrypted after noise disturbance and weights adding. What the SP can get are the ciphertexts. On one hand, the SP can verify each user's signature and the source of each ciphertext. So it can prevent the group users from maliciously forging the fake ciphertexts and wasting the computation and network resources. On the other hand, because the SP does not have the user's private key, it cannot complete the decryption to get the location of each user. Moreover, each user can get none of the other users' locations. After obtaining the group center, all the users make service requests with the center location as the anchor point. Therefore, both the location privacy-protection of the group and the location privacy-protection of every individual user in the group can be realized.

In the group, the users use p_1's public key to encrypt their own coordinates after adding noise and weights; it is impossible to decrypt the ciphertexts of p_1 to obtain his location. Even $p_2, \cdots, p_k$ collude with the SP; they cannot guess the location of p_1, because they do not have the private key of p_1.

In another case, if p_1 colludes with other $l(l < k-2)$ users in the group, because $k-(l+1) > 1$ is established, the colluded users can only get the sum of at least two users' location data. Additionally, the data of noise and weights have been added, respectively. It is impossible to guess either specific location of the rest of users in the group. Therefore, the scheme in Section 4.1 can resist the collusion attack of most users in the group.

Particularly, we have the collusion between p_1 and the SP. The collusion can only be realized by providing p_1's private key directly to the SP for decryption of all the ciphertexts. In this case, the security of p_1's own location privacy and other encryption related applications will be seriously threatened. So, for his own benefit, p_1 would not like to choose this way to collude with the SP. The other case is that p_1 still keeps his private key secret. Instead, the SP provides all the other users' ciphertexts received to p_1. p_1 decrypts the ciphertexts of other users' locations and shares the locations with SP. In this case, it cannot be ignored that the SP has the group center, which is computed from all the users' real locations. It can infer the location of p_1 according to all the rest of the users' locations and the center location, which is also unacceptable for p_1. So this collusion case may lead to a paradox of the users' original intention of location privacy-preserving and the threat of his location privacy security. Hence, combining with the game theory of the collaborative position privacy-protection [22], the probability of collusion between p_1 and the SP is negligible. In conclusion, the scheme in Section 4.1 can resist the collusion attacks.

(2) Similarly, in the scheme of Sections 4.2 and 4.3, the processes of calculation for the best set position and the group friend's distance also need the users in the group to encrypt their disturbed and weighted location data. Then the ciphertexts are sent to the SP to get outsourced and aggregated computation. After receiving and decrypting the processed result from the SP, the user can obtain the best collection location for the group and the friend's distance, respectively. Their privacy security proofs are similar to that of the scheme in Section 4.1, which realize not only the group's location privacy protection but also the users' location privacy protection within the group. They can also resist the collusion attacks. Here it is not necessary to repeat the detailed demonstration.

Table 2: Characteristics comparison.

Scheme	[3]	[4]	[5]	[6]	Ours
Method	Distance sum	Center location	Center location	Center location	Center location
Network resources occupied	Low	Low	Low	High	Low
The size of the service result set	$o(n)$	$o(1)$	$o(1)$	$o(1)$	$o(1)$
Resistance against the collusion attack between SP and m users	$m = 0$	$m = 1$	$1 \le m < k - 1$ or $m = 1$ (with or without the special proxy user)	$1 \le m < k - 1$	$1 \le m < k$
Controllability of the location privacy protection	Fine-granularity	Coarse-granularity	Coarse-granularity	Coarse-granularity	Fine-granularity
Communication mode	Ring-unicast	Ring-unicast	Star-unicast	Group-broadcast	Star-unicast
User state	Static	Static/dynamic	Static/dynamic	Static	Static/dynamic

(3) In the dynamic user group queries, the position of p_1 is changing every time as he makes a new query request. Because the position of p_1 is always changing, even if the attacker can pretend to be the other users in the group to obtain the distances from p_1 through multiple requests, the specific position coordinates of p_1 cannot be determined yet. Therefore, this scheme can resist the existing distance interaction attack [3]. □

5.3. Characteristics Analysis. As shown in Table 2, we will compare the related schemes with ours. In our schemes, the users in the group conduct the encryption in parallel, which brings the high efficiency. The SP performs the outsourcing calculations on the ciphertexts without knowing the real locations of each user. The SP's strong computation capability is in full use in our method. Moreover, the user can obtain the query service result by only a simple decryption operation.

Both of the schemes in [3, 15] adopt the method of computing the distance sum to obtain the group center and need to get the candidate target locations and each user's anonymous region in advance. Taking [3] as an example, the number of the query nodes is the number of the users in the group. The SP returns a set of candidate target locations, which needs a filtering algorithm to get the exact target location from the set. Compared with our privacy-protection scheme of GNN query, they bring additional overhead. Meanwhile, the distance leakage may threaten the privacy of the user's location in the group. References [3, 15] ignore the collusion attacks in their schemes.

Additionally, the schemes in [4, 6] also cannot resist the collusion attack between the SP and the multiple users of the group. Both [5] and our method safely calculate the center position of the user group to carry out the GNN query, converting the GNN query problem to the NN query problem. Thus, the number of the query points is only one, that is, the group center. The result of query is certain. There is no need for any added filtering algorithm for selection.

In addition, GLP protocol [6], the schemes in [5], and our paper all use cryptographic algorithms for location privacy-protection. However, the former requires each user in the group to broadcast the messages to other users for precomputation, which occupies much more network resources than the unicast way of communication in our paper. The latter uses Paillier algorithm based on secret sharing to compute the center location. Although the collusion attack is considered in [5], the collusion attack between the proxy user and the SP cannot be resisted at all. The proxy user is essentially the same as the center server we do not want. It is also the performance bottleneck of the protection system. Compared with our scheme, neither of schemes in [5, 6] takes into account the collusion between the SP and all the users of the group. Moreover, their computation cost is larger, and the users in the group cannot measure or control the degree of privacy protection and the quality of query services.

In the single group query service, the scheme proposed by us only needs the users to encrypt their respective disturbed locations once. If the complexity of the signature algorithm is ignored, the computation time complexity is $o(\sqrt{T})$. It is equal to the complexity of BGN encryption. In the three different application scenarios of LBSs, the users' mobile terminals only need to separately calculate once for the ciphertexts of their own coordinates, and the encryption of each user can be highly parallel processing. Particularly, because only the user who initiates the query service needs to perform the decryption algorithm to get the group center, his computation complexity is $o(2\sqrt{T})$. It is the computation complexity of the encryption and decryption algorithms of BGN cryptosystem.

The main computation of the SP is the aggregation of all the ciphertexts from k users. Because the ciphertexts are integers in BGN cryptosystem, in simple terms, the complexity is equal to the multiplication of k integers. Furthermore, the aggregation can also be carried out efficiently by parallel multiplication so as to reduce the waiting time of response. In addition, the communication cost mainly comes from the k ciphertext messages sent by the individual users in star-unicast mode and the broadcast message for informing the group center. In conclusion, compared with the related

classic researches, our method has less computation and communication overheads in general.

6. Conclusion

Combined with the research status of the location privacy-protection schemes in LBSs, there are still some problems to be solved urgently. Fortunately, these problems have been mainly solved in our paper.

(1) Centralized structure depends on the central anonymous server. As it is doubted for reliability, performance bottleneck, weak antiattacking capability, and other problems, it is easy to cause the leakage of user's location privacy and influence the quality of location service.

(2) Privacy protection is mainly applied to the individual user, and less consideration is given to the group location privacy-protection of multiple users that are also practical in the reality.

(3)Users not only want to share other users' net resources to obtain better LBSs and achieve privacy protection but also do not want to reveal their own location information to others.

(4)The degree of privacy protection cannot be quantified or measured, which means that the effects of privacy protection are transparent to the users, and they cannot realize flexible setting and fine-grained control.

Our contributions are as follows: based on BGN cryptographic algorithm, three group location privacy-protection schemes of distributed structure are, respectively, proposed according to the classic application scenarios in LBSs, which are GNN query, the best group gathering location query, and the group friend's distance query services, achieving k-anonymity without anonymous regions. Based on the special privacy homomorphism of BGN cryptosystem, the users encrypt the disturbed and weighted location data for only one time; then the ciphertexts are outsourced and calculated by the SP to obtain a corresponding aggregated result to the three different application scenarios mentioned above. So only one security policy is used; namely, the BGN algorithm is performed only once. It can solve the group location privacy-protection problem in three typical applications in LBSs simultaneously without exposing any group user's location. Compared with the existing related research results, the analysis proves that the proposed method has a wider range of applications and is more flexible. Users can change the weighting parameters to affect the group center according to the quantitative indicators. The weight sequence is introduced to make it possible to dynamically adjust the influence and contribution of each user's real location to the group center for realizing fine-granularity control of the effects of the group location privacy-protection. At the same time, it has better performance and can ensure secure and efficient group location privacy-protection in LBSs with lower communication and computation complexity. Furthermore, our schemes can also resist the distance interaction attacks and collusion attacks.

Data Availability

The conclusion of our paper is based on the mathematical and cryptotheorem. If the specific examples to verify the findings of our study are needed, anyone would be welcome to contact the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant No. 61572521, the National Natural Science Foundation of China under Grant No. U1636114, and the National Key Research and Development Program of China under Grant No. 2017YFB0802000.

References

[1] A.-Y. Zhou, B. Yang, C.-Q. Jin et al., "Location-based services: architecture and progress," *Chinese Journal of Computers*, vol. 34, no. 7, pp. 1155–1171, 2011.

[2] Y. Huang, Z. Huo, and X.-F. Meng, "Coprivacy: a collaborative location privacy-preserving method without cloaking region," *Chinese Journal of Computers*, vol. 34, no. 10, pp. 1976–1985, 2011.

[3] T. Hashem, L. Kulik, and R. Zhang, "Privacy preserving group nearest neighbor queries," in *Proceedings of the 13th International Conference on Extending Database Technology: Advances in Database Technology - EDBT 2010*, vol. 426, pp. 489–500, Switzerland, March 2010.

[4] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Computer Communications*, vol. 31, no. 6, pp. 1181–1191, 2008.

[5] G. Sheng, M. JianFeng, Y. QingSong et al., "Towards cooperation location privacy-preserving group nearest neighbor queries in LBS," *Journal on Communications*, vol. 36, no. 3, pp. 54–62, 2015.

[6] M. Ashouri-Talouki, A. Baraani-Dastjerdi, and A. Aydin Selcuk, "GLP: a cryptographic approach for group location privacy," *Computer Communications*, vol. 35, no. 12, pp. 1527–1533, 2012.

[7] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[8] Y.-H. Wang, H.-L. Zhang, and X.-Z. Yu, "KAP: Location privacy-preserving approach in location services," *Tongxin Xuebao/Journal on Communication*, vol. 35, no. 11, pp. 182–190, 2014.

[9] K. Geng, F. Li, W. Li et al., "Proxy-based privacy-preserving scheme for mobile internet," *Journal on Communication*, vol. 36, no. 11, pp. 26–32, 2015.

[10] M. L. Yiu, C. S. Jensen, X. Huang et al., "SpaceTwist: managing the trade-offs among location privacy, query performance ,and query accuracy in mobile services," in *Proceedings of the IEEE 24th International Conference on Data Engineering (ICDE '08)*, pp. 366–375, IEEE Press, Cancun, Mexico, April 2008.

[11] W. Ni, M. Gu, and X. Chen, "Location privacy-preserving k nearest neighbor query under user's preference," *Knowledge-Based Systems*, vol. 103, no. 2016, pp. 19–27, 2016.

[12] Z. Feng, H. Tan, and H. Shen, "Relationship privacy protection for mobile social network," in *Proceedings of the 4th International Conference on Advanced Cloud and Big Data, CBD 2016*, pp. 215–220, China, August 2016.

[13] Z. Cai, Z. He, X. Guan et al., "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 99, pp. 1–14, 2017.

[14] Y. Huang, Z. Cai, and A. G. Bourgeois, "Search locations safely and accurately: a location privacy protection algorithm with accurate service," *Journal of Network and Computer Applications*, vol. 103, no. 2018, pp. 146–156, 2018.

[15] Y. Huang and R. Vishwanathan, "Privacy preserving group nearest neighbour queries in location-based services using cryptographic techniques," in *Proceedings of the GLOBECOM 2010 - 2010 IEEE Global Communications Conference*, pp. 1–5, Miami, Fla, USA, December 2010.

[16] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in *Proceedings of the Advances in Cryptology (AsiaCrypt)*, vol. 1716 of *Lecture Notes in Computer Science*, pp. 165–179, Springer, 1999.

[17] F. Hao and P. Zieliński, "The power of anonymous veto in public discussion," in *Transactions on Computational Science IV*, vol. 5430 of *Lecture Notes in Computer Science*, pp. 41–52, Springer, Berlin, Germany, 2009.

[18] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proceedings of the Theory of Cryptography, TCC'05*, vol. 3378 of *Lecture Notes in Computer Science*, pp. 325–341, Springer, 2005.

[19] Y. Xun, R. Paulet, and E. Bertino, *Homomorphic Encryption and Applications*, Springer, 2014.

[20] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169–180, 1978.

[21] A. K. Tyagi and N. Screenath, "A comparative study on privacy preserving techniques for location based services," *British Journal of Mathematics & Computer Science*, vol. 10, no. 4, pp. 1–25, 2015.

[22] C. Y. Feng, L. X. Jun, and L. Bin, "Collaborative position privacy protection method based on game theory," *Computer Science*, vol. 40, no. 10, pp. 92–97, 2013.