A Blind Signature-based Location Privacy Protection Scheme for Mobile Social Networks

Xin Xu, Mi Wen, and Liangliang Wang
(Corresponding author: Xin Xu)

College of Computer Science and Technology, Shanghai University of Electric Power
Shanghai, 200090, China
Email: 18108035@mail.shiep.edu.cn

(Received June 6, 2020; Revised and Accepted Feb. 10, 2021; First Online Aug. 14, 2021)

Abstract

Location-based services (LBS) have gradually become an integral part of people's lives. In mobile social networks, we hope to protect our location privacy information in different environments and get services in time. However, scholars have proposed various effective location privacy protection strategies, such as k-anonymity, fuzzy location, etc. However, these privacy protection technologies are based on the location information obtained, and it is rarely achieved from the stage of location acquisition. In this article, we propose a privacy protection scheme based on blind signatures [9] for mobile locations. The solution uses a blind signature and pseudonym to verify the user's identity anonymously. It adds false information to form k-anonymity, which can flexibly protect the user's relevant information in different environments and achieve the two-stage privacy protection of LBS. Simulation results show that this method has better performance and higher security compared with other existing approaches, and it can be applied to different types of mobile environments.

Keywords: Blind Signature; Location Privacy Protection; Mobile Social Networks; User Collaboration

1 Introduction

With the popularity of mobile devices, LBS has become an essential part of human life. It is widely used in all aspects of people's lives and bring great convenience to people. For example, when we are chatting with our friends, we could send our own location information to them for sharing our life. We can also send our location information to the relevant application to get the local weather, and plan the perfect route information for travel. Unfortunately, when we enjoy the convenience of LBS, we also face some challenges. If the service provider is untrusted, it may leak the user's location information. Some attackers can further steal users' privacy data (such as salary and bank card number) based on users' location information and social engineering, so as to obtain more benefits from targeted attacks [1, 8, 15, 24, 27].

The LBS mainly contains two stages:

1) Location acquisition stage: The stage where the mobile device acquires its current location through GPS or a third-party network.

2) Service acquisition stage: The stage in which the mobile device sends the location information and the inquired points of interest to the LBS provider, and the LBS provider performs the inquiry and returns the service information to the mobile device [5].

As shown in Figure 1. Unfortunately, the existing privacy protection methods of LBS cannot be applied to both stages of LBS at the same time. In the service acquisition phase, the user directly submits their location information, and privacy protection technology enables the LBS provider to provide users with corresponding services without knowing the user's exact location by anonymization and generalization of the location information [14, 23, 25]. While in the location acquisition phase, the user submits the current location fingerprint, and the Location Provider(LP) estimates the specific location based on the fingerprint [11,17,20], but the location fingerprint represents a definite location, which cannot be processed by obfuscation technology.

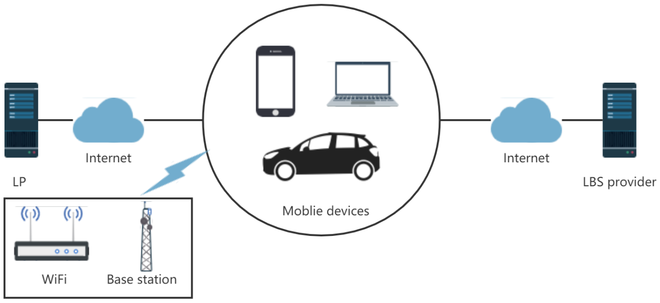


Figure 1: Location-based service architecture

In mobile social networks, we hope to be able to obtain services in time while protecting location privacy. However, since users may be in different environments and scenarios, the demand for anonymity levels may also be different [21]. If we use the same level of privacy protection methods, it may affect the quality of the service, such as the real-time nature of the message; it may also affect the strength of privacy protection, such as the confidentiality of data and the anonymity of user identity and location [22]. To solve the above problems, this paper proposes a mobile location privacy protection scheme based on a blind signature [7]. At the same time, the combination of k-anonymity and virtual information technology enables the solution to be implemented flexibly according to the number of users in the collaboration group. Therefore, the security of the solution will not vary greatly in different environments.

Our main contributions are listed as follows:

1) In order to fully protect the privacy of the two stages of LBS, we study the similarity of information transmission between the two stages, and use blind signature technology to separate the user identity and related request information, so as to achieve location privacy protection of both stages of LBS.

2) Secondly, we use k-anonymity and false information to protect the location information and keep the diversity of requested information according to the needs of users and the differences in the surrounding environment.

3) Thirdly, we analyze the security strength and privacy protection capabilities of BSLPP (Blind Signature-based Location Privacy Protection). In particular, we use provable security technology to formally prove that it is safe to protect users' private information under man-in-the-middle attacks. Through performance analysis, we prove that BSLPP is indeed more effective than the scheme mentioned in [16,18]. Compared with the scheme mentioned in [11], the safety and applicability of our scheme have also been improved.

The rest of the paper is organized as follows: Related work is reviewed in Section 2. We introduce our system model, security requirements, and our design goal in Section 3. In Section 4, we introduce our scheme design. Section 5 shows the security analysis of the scheme. Section 6 conducts performance evaluation. We conclude this paper in Section 7.

2 Related Work

For the protection of the third LP's privacy, Damiani and Cuijpers [2] first pointed out that when users use the third-party network location, the user will submit the information of nearby access points(APs) to the third-party LP, and the LP will calculate the location information. In this case, the LP will obtain their location information before the user, which causes the user's location information to be leaked. Sun *et al.* [11] used homomorphic encryption to perform location processing in the ciphertext space to prevent the access point information in the service from being threatened by privacy. However, the balance between system overhead and quality of service has become a disadvantage of this solution. Wang *et al.* [20] proposed a method to add virtual information to the location request so that the location server cannot distinguish the user's real location information from the virtual information. However, the virtual location generated by this strategy may be recognized by the location server, which greatly reduces the security of the solution. Song *et al.* [17] applied the location privacy protection strategy to complete fingerprint matching on the client. In this approach, the client matches its location fingerprint with the fingerprint data received within this range to obtain its location information. But the fingerprint data received in this range is provided by LP, it still knows the location range of the client, so the protection of user identity and specific location is not high.

In the service acquisition phase, in order to deal with untrusted third-party anonymous servers, Peng *et al.* [14] added a function generation server on the basis of the anonymous server structure to aggregate users with the same value to achieve k -anonymity. In addition, scholars have also proposed techniques that combine k-anonymity with other technologies, such as autonomous learning [13] and clustering [26]. Ye *et al.* [23] introduced pseudo-queries in LBS query requests to effectively resist query probability statistical attacks and continuous attacks, and prevented attackers from mapping the specific content of query requests based on user identity. Zhao *et al.* [25] combined user privacy with geographic location information, and generated corresponding fake locations to protect user privacy based on the user's different access probabilities to different points of interest. In order to obtain higher query accuracy and privacy protection level, there are still some works are based on the cryptographic techniques [10,28]. Liao *et al.* [12] pointed out Qi's registration agreement [4] may not delete the linkability of the real ID and authorized anonymous ID, so they proposed an improved registration and re-obfuscation protocol that prevented administrators from obtaining unauthorized anonymity and true identity. Maede *et al.* [18] proposed a new privacy protection protocol by using blind signature technology. Instead of excessively protecting the user's ID, they encrypted the query information to achieve user identity and security. The separation of messages protects the user's location privacy, but once the database colludes with others to leak the shared key, it will the user's identity be misused to make illegal queries. Researchers also proposed differential privacy technique [3,6,19] to protect the user's location information. However, all of these solutions are bringing a large computation burden on the user side, which makes it is not suitable for mobile devices. Junggab *et al.* [16] developed a location privacy protection strategy based on pseudonyms. He functionalized the pseudonyms and used secret sharing technology to share locations with designated friends, giving a lot of calculations to the service is more suitable for mobile social networks, but server failure is still the bottleneck of the solution.

3 System Model, Security Requirements and Design Goal

In this section, we formalize the system model, system design goal, and system security requirements. This paper adopts a distributed peer-to-peer model, and proposes an untrusted environment-oriented architecture consisting of mobile users, LP, and LBS providers. The architecture and message flow are shown in Figure 2.

3.1 System Model

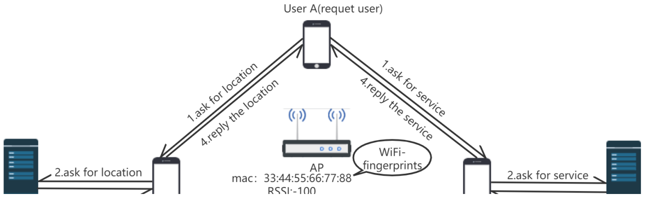


Figure 2: System model

Mobile User: It can communicate with other users or servers through the AP. The mobile user may be a user requesting a service or a member of a collaboration group. As a user requesting a service, he interacts with members of the collaboration group and lets them initiate requests to the server instead of himself. As members of the collaboration group, they interact with the server on behalf of users who request services, complete location queries and LBS requests, and return the results of the requests to users who request services.

AP: APs provide communication channels for collaborative users, WiFi fingerprints for users who need them, and basic information for the location.

LP: The LP calculates location information based on the Wi-Fi fingerprint sent by the user, and returns the location result to the corresponding user.

LBS Provider: The LBS provider returns the corresponding service information to the user based on the location provided by the user and the requested service.

3.2 System Security Requirements

Security is critical to the success of location privacy protection. In our security model, we consider that the LP and the LBS provider are untrusted, and those collaborative users are also at risk of leaking information. First, we send location-related information and request types to the LPs and the LBS providers, who may leak our related privacy information to criminals. For collaborative users, they may also be mixed with attackers, and cooperate with other collaborative users to modify our information or analyze it through space-time correlation analysis to leak our private information. In addition to the above two types of insecure factors, there are also man-in-the-middle attacks and analyze attacks launched against us by external attackers. Therefore, in order to prevent the above-mentioned insecure factors, the following security requirements should be satisfied in the process of location privacy protection.

The Data Confidentiality. Protect personal location privacy-related information from attackers, that is, even if communication is eavesdropping during collaboration, the content of the message cannot be identified. In this way, the user's privacy data protection can be satisfied.

The Anonymity of the User's Identity and Location. Even if the LPs and LBS providers get the real location information and the requested content, they cannot distinguish which user it comes from.

Authentication and Data Integrity. Authenticate the encrypted information sent by legitimate cooperative users that have not been tampered with during transmission, that is, if an attacker forges and/or modifies information, malicious operations should be detected. The collaborator only completes the corresponding service for receiving correct and credible messages.

3.3 Design Goal

Under the above system model and security requirements, our design goal is to provide a location-based service with strong applicability, high security and responsiveness. Specifically, the following two goals should be achieved.

Suitable for Various Environments. Due to the mobility of users, we may be in a sparsely populated area, so the confidentiality of some privacy protection algorithms may be greatly reduced. We want to protect our location privacy wherever we are.

Ensure the Safety and Timeliness of Services. We want users' privacy not to be known to anyone, even collaborative users. On the basis of ensuring security, we also hope that it will not affect the user's service experience.

4 The Proposed BSLPP Scheme

This paper protects the privacy of the user's location by user collaboration, and gets rid of the bottleneck of using anonymous servers. The solution is divided into three parts including establish an anonymous collaborative group, protect the privacy of location services, and protect the privacy of LBS. Table 1 lists the notations used throughout the description of the scheme for ease of reference.

Table 1: Notation

U_A	Mobile user A
$ID_{A_{num}}$	Pseudonym calculated using the MAC of user A
k	The number k of anonymity
k_{min}	the minimum value of k that meets the need for anonymity
R	The number of hops in the anonymous zone
$H(m)$	Hash message m
MAC_{other}	Client's hardware address
$Figure_{num}$	A WiFi fingerprint
$r_{A_{num}}$	A random number generated by user A
t_{num}	Timestamp to prevent replay attacks
$Location_{num}$	A series of location information
$Type_{num}$	Multiple types of request services
S_{L-P}	Provider of location
S_{LBS-P}	Provider of LBS
$PubK_A$	Public key pair of user A
$PriK_A$	Private key pair of user A
$\{m\}_{PubK_A}$	Encrypt message m with the public key of user A
$\{m\}_{PribK_A}$	Sign message m with the private key of user A
K_{AB}	Shared secret key between users A and$B$
$\{m\}_{K_{AB}}$	Encrypt message m with the secret shared key K_{AB}
$C(x)$	Blind message x
$C^{-1}(x)$	Unblind message x

4.1 Establish Anonymous Collaborative Group

Our solution uses a point-to-point communication method and establishes a k-anonymous collaboration group to prepare for the next service acquisition. We describe the proposed scheme as follows.

1) User A asks whether users within the R-hops range are willing to participate in collaborative work through broadcasting.

2) If the user agrees to cooperate, the user who receives the request message sends the reply to user A with his public key, user identifier ID and hops R' from user A. If they does not agree, user A ignores this message.

3) After receiving $2k$ user's replies, user A selects k users arbitrarily, lists them (user identifier, user public key, recent usage times, and hop count). If the number of users receiving the reply is less than k and greater than k_{min}, randomly select n ($n < k$) users, and add k-n messages as dummy messages from the recent historical query information. If the number of users who received the reply is less than k_{min}, expanded hop count R and continue to repeat 1) - 2).

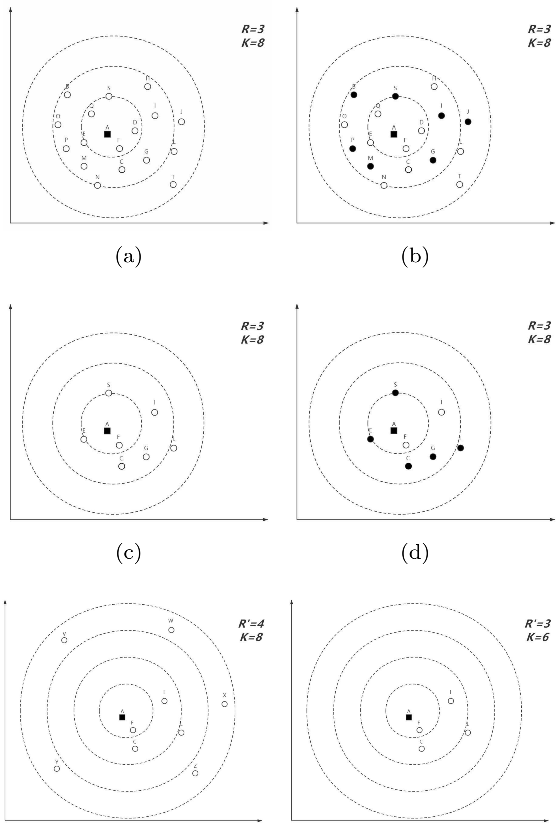
4) In the next query, if the difference between the number of hops with the collaborating user is less than R, the interaction continues. If the difference is greater than R, then user A deletes the corresponding user in the list to save time and costs. After deletion, if the number of collaborative users is less than k, please repeat 1) -3).

The pseudo code of establishing anonymous collaborative group is elaborated in Algorithm 1.

Algorithm 1 Establish anonymous collaborative group

```
1: $U_A \rightarrow U_{other}$: request for the collaborative work within the range of hops $R$
2: if $U_{other}$ agree then
3:     Compute $ID_{other}$=$H(MAC_{other})$*$r_{other_1}$+$r_{other_2}$;
4:     Send $\{ID_{other}, PubK_{other}, H(ID_{other}, PubK_{other})\}$ to $U_A$;
5: end if
6: if the number of users exceeds $2k$ then
7:     Select $k$ users randomly in $2k$ users and add $\{ ID_{other}, PubK_{other}, R \}$ into list $L$;
8: end if
9: if the number of users less than $k$ and exceeds $k_{min}$ then
10:    Select $n$ users randomly, and $k$-$n$ messages in the historical query information.
11: end if
12: if the number of users less than $k_{min}$ then
13:    Expanded hop count $R$ or reduce $k$ and return step 1;
14: end if
15: while their collaboration distance differs by more than $R$ do
16:    Delete the corresponding user from list $L$;.
17:    if the number of cooperative users is less than $k$ then
18:        Return step 1
19:    end if
20: end while
21: End
```

Figure 3 shows the step of establishing an anonymous collaborative group, where user A executes the algorithm. The transmission range of user A is represented by a dotted circle. User A sends a broadcast request for collaboration, and then receives *16* near peers represented by white circles (Figure 3(a)). User A then randomly selects *8* collaborative users represented by black dots and add them in list L(Figure 3(b)). But user A receives the number of near peers represented by white circles less than *8* and exceeds *4* (Figure 3(c)). User A then randomly selects *5* collaborative users represented by black dots and add them in list L and sends *3*different messages in the next service request algorithm (Figure 3(d)). When the number of received replies is less than *4*, expand the number of hops of the route or reduce the number of anonymities as required (Figure 3(e)- 3(f)).



(a) (b)

(c) (d)

(e) (f)

Figure 3: Components of an anonymous collaboration group

4.2 Protect the Privacy of Location Service

To ensure that users obtain the privacy of their location through the network. On the one hand, we use blind signature technology to blind the WiFi fingerprint information, so that the user's identity is separated from the request. On the other hand, we mix some dummy location information to confuse the sight of the collaborative users and LPs, but also make the solution available in sparsely populated places.

1) User A sends a WiFi fingerprint request to the surrounding collaborative users.

2) The collaborative user randomly selects zero to three WiFi fingerprint information around him, signs and sends it using his private key to user A.

3) User A receives the message and verifies it with the corresponding public key, and records it as $Figure_1$, $Figure_2$...

4) Then user A randomly selects a user in a collaboration group and records the most recent trials in his list, such as user B. User A uses his pseudonym ID_{A_1} to send his public key and blinded WiFi fingerprint information to user B. To ensure security, the fingerprint information here may be mixed with WiFi fingerprints requested from other users. Even if someone queries the location through the location server, they don't know if it is the user's real location.

5) User B authenticates the sent message. If the verification is successful, the blinded message is signed, otherwise the request from user A is rejected.

6) User A verifies the message that sent back. If the verification is successful, the message is unblinded. Otherwise, ignore the message and reselect a new user, repeat 4).

7) User A encrypt the message that including the query request, the signed and unblinded message and session key with User B's public key and sends to User user B using pseudonym ID_{A_2}.

8) After received the message, user B decrypts and verifies the validity of the signature. If the verification is passed, the location information query is performed on behalf of the user A, otherwise the request is rejected.

9) User B submits the fingerprint information to the LP, and the LP performs calculation based on the fingerprint information and returns the location information to user B. User B encrypts the result and the signed and unblinded message with the session key, then returns it to user A.

The pseudo code of protecting the privacy of location service is elaborated in Algorithm 2.

4.3 Protect the Privacy of LBS

In terms of obtaining location-based services, we must not only consider protecting user location information, but also protect the type of information requested. Because some users are more sensitive to where they are and some users pay more attention to the type of message requested. Therefore, we have taken these two points into consideration while integrating the privacy protection of location services to provide users with more comprehensive protection.

1) User A randomly selects users where except user B in a collaboration group, such as user C. And records the most recent trials of user C in his list. User A uses his pseudonym ID_{A_3} to send his public key and

Algorithm 2 Protect the privacy of location service

```
$U_A \rightarrow U_{other}$: request for the WiFi fingerprint
if $U_{other}$ agree then
    Send $M_1 = \{ Figure, t_1, m_1 = \{ Figure\}_{PriK_{other}}\}$ to $U_A$;
end if
if $\{m_1\}_{PubK_{other}} == Figure$ is (TRUE) then
    $U_A$ add it in list $FP$;
end if
$U_A$ computes $x$=$H(Q$=$(Figure_1,Figure_2,...,Figure_n)$ to $ID_B$;
$U_A$ sends $M_2$=$\{ ID_{A_1}, PubK_A, t_2, C(x), m_2$=$\{ H(ID_{A_1},t_2,C(x), PubK_A)\}_{PriK_A}\}$ to $ID_B$;
$U_B$ decrypts $\{m_2\}_{PubK_A}$
if H$(ID'_{A_1}, PubK'_A, t'_2,C(x)) == m_2$ is (TRUE) then
    $U_B$ sends $M_3$=$\{ ID_B, t_3, m_3 = \{C(x)\}_{PriK_B} \}$ to $ID_{A_1}$;
end if
if $\{m_3\}_{PubK_B} == C(x)$ is (TRUE) then
    $U_A$ unblinds $s = C^{-1}(m_3)$ and sends $M_4$=$\{ ID_{A_2}, t_4, m_4$ =$\{ ID_{A_2}, t_4, s, Q, K_{AB}\}_{PubK_B}\}$ to $ID_B$;
end if
$U_B$ decrypts $\{m_4\}_{PriK_B}$
if $H(Q') == \{s'\}_{PubK_B}$ is (TRUE) then
    $U_B$ sends $Q$ to $S_{L-P}$;
end if
After received $\{Result\}$ from $S_{L-P}$, $U_B$ sends $\{Result, s\}_{K_{AB}}$ to $ID_{A_2}$.
End
```

blinded request information based on location services to user C. In order to meet the demands of different users, we propose two formats of request information here. When the user is in a sensitive location, he sends a collection of locations containing other nearby locations. When the user requests a more sensitive message type, he sends a collection of information of multiple request types.

2) User C authenticates the sent message. If the verification is successful, the blinded message is signed. Otherwise the request from user A is rejected.

3) User A verifies the message that sent back. If the verification is successful, the message is unblinded. Otherwise, ignore the message and reselect a new user, repeat 1).

4) User A encrypt the message that including the query request, the signed and unblinded message and session key with user C's public key and sends to user C using pseudonym ID_{A_4}.

5) After received the message, user C decrypts and verifies the validity of the signature. If the verification is passed, the location information query is performed on behalf of the user A, otherwise the request is rejected.

6) User C submits the request information to the LBS provider, and the LBS provider returns a result set based on the requested information to user C. User C encrypts the result and the signed and unblinded message with the session key, then returns it to user A.

The pseudo code of protecting the privacy of LBS is elaborated in Algorithm 3.

Algorithm 3 Protect the privacy of LBS

```
$U_A$ computes $y$=$H(Q$=$(Location_1, Location_2, ..., Location_n, Type)$ or $Q$=$(Type_1,Type_2, ...,Type_n, Location)$) to $ID_C$;
$U_A$ sends $M_5$=$\{ ID_{A_3}, PubK_A, t_5, C(y), m_5$=$\{ H(ID_{A_3}, t_5,C(y),$
    to $ID_C$
$U_C$ decrypts $\{m_5\}_{PubK_A}$
if $m_5 ==$ H$(ID'_{A_3}, PubK'_A, t'_5,C(y))$ is (TRUE) then
    Send $M_6$=$\{ ID_C, t_6, m_6$=$\{C(y)\}_{PriK_C} \}$ to $ID_{A_3}$;
end if
if $\{m_6\}_{PubK_C} == C(y)$ is (TRUE) then
    $U_A$ unblinds $s = C^{-1}(m_6)$ and send $M_7$=$\{ ID_{A_4}, t_7, m_7$=$\{ ID_{A_4}, t_7, s, Q, K_{AC}\}_{PubK_C}\}$ to $ID_C$;
end if
$U_C$ decrypts $\{m_7\}_{PriK_C}$
if $H(Q') == \{s'\}_{PubK_C}$ is (TRUE) then
    Sends $Q$ to $S_{LBS-P}$;
end if
After received $\{Result\}$ from $S_{LBS-P}$, $U_C$ sends $\{Result, s\}_{K_{AC}}$ to $ID_{A_4}$.
End
```

For security reasons, users must use different collaborative users to serve them during two different queries. After the user's identity as a request service and a collaboration service is converted, he must be using different public-private key pairs. In order to prevent correlation attacks and analysis attacks based on historical information, users often need to maintain and change their public and private keys.

5 Security Analysis

In this section, we will analyze the security of the proposed BSLPP scheme. In particular, according to the security requirements discussed earlier, our analysis will focus on data confidentiality and anonymity of user identities, and authentication and data integrity.

1) The confidentiality of data and anonymity of user identities are achieved in the proposed BSLPP scheme. In the proposed BSLPP scheme, when the user sends request information to the collaborating user, the information Q is first hashed to form $x = H(Q)$, and then the summary information x is

blinded as follows:

$$\begin{aligned} C_1 &= r_1 * x^a \\ C_2 &= r_2 * x^b \end{aligned} \tag{1}$$

After receiving the encrypted blind message, the collaborative user first decrypts the private key to obtain C_1, C_2, and then signs C_1, C_2 as follows::

$$\begin{aligned} C_1' &= {C_1}^d \bmod n \\ C_2' &= {C_2}^d \bmod n \end{aligned} \tag{2}$$

After the user obtains the signed data C_1', C_2', he unblinds it as

$$\begin{aligned} S_1 &= C_1' * {r_1}^{-1} \bmod n \\ S_2 &= C_2' * {r_2}^{-1} \bmod n \\ S &= {S_1}^k * {S_2}^l \bmod n \end{aligned} \tag{3}$$

accroding to Equations (1) (2) (3), we can get Equation (4)

$$\begin{aligned} S^e &= {S_1}^k * {S_2}^{l^e} \bmod n \\ &= ((C_1' * {r_1}^{-1})^k * (C_2' * {r_2}^{-1})^l)^e \bmod n \\ &= (({C_1}^d * {r_1}^{-1})^k *, ({C_2}^d * {r_2}^{-1})^l)^e \bmod n \\ &= (x^{d*(ak+bl)})^e \bmod n \\ &= (x^d)^e \bmod n \\ &= x \bmod n. \end{aligned} \tag{4}$$

On the one hand, the user obtains the signature data of the collaborative user without disclosing the content of the request message; on the other hand, even if the user publishes the signature, the collaborative user cannot track the signature data. Because the collaborative user retains a set of data (C_1, C_2, C_1', C_2'), but he has no way to know (r_1, r_2, a, k, b, l) from S. In the two interaction phases of request signature and request service, users use different pseudonyms and public and private keys to interact with the collaborative user, so the collaborative user cannot associate the original request data Q with the user's identity. Thus, the confidentiality of data and anonymity of user identities is achieved between users and collaborative users.

2) The authentication and data integrity of between users and collaborative users are also achieved in the proposed BSLPP scheme. In the proposed BSLPP scheme, The user sends the signed data together with the original data to the collaborating user. The collaborating user first hashed to form $x_i' = H(Q_i')$, then sign the formed abstract to get S_i'. Compare S_i' with S_i. If they are the same, they are the users who have completed the signature before, and thus complete the identity verification as users in the collaboration group. In each information exchange process, we hash the message. If the data is changed, we will easily find out. Since then, the integrity of the data has been verified.

6 Performance Evaluation

In this section, we evaluate the performance of our framework in terms of computation cost on the involved parties as well as the communication cost. The main computation operations in our scheme include exponentiation and multiplication in G and GT, and pairing, besides, it also contains the symmetric and the asymmetric encryption and decryption cost. Table 2 presents the meaning of notations used in this section.

Table 2: Notations used in the performance evaluation

Notations	Description
M	The number of records which satisfies the original query
N	The number of information in the server
N'	The number of information submitted
T_{LE}	The time of lagrangian interpolation construction
T_{LD}	The time of lagrangian interpolation decryption time
T_{SE}	The time of symmetric encryption
T_{SD}	The time of symmetric decryption
T_{BM}	The time of blind message
T_{UM}	The time of unblind message
T_{PE}	The time of RSA encryption
T_{PD}	The time of RSA decryption
T_p	The time of pairing
${T_e}^G$	The time of exponentiation in group G
${T_m}^G$	The time of multiplication in G

6.1 Efficiency Analysis

In this section, we introduce the calculation and communication comparison between [11, 18] and our scheme. Since [11, 18] are two different stages in LBS, we will compare the stages corresponding to our scheme with them separately. For simplicity, we have omitted some fixed costs in all three frameworks. See Table 3 for details.

In [11], the system uses a client-server model, so there is no agent consumption. The cost of the client is the number of APs collected in the current building and the exponentiation and modular multiplication of homomorphic encryption and decryption costs. The cost of the server lies in the number of APs submitted in the database and the exponentiation and modular multiplication of the state encryption and decryption costs.

The calculation cost on the user side depends only on the number of POI records that satisfy the original query. Compared with the third part of our framework, the computational cost of the user side in [18] saves one public key encryption time; But in terms of the computational cost on the agent. in [18], it needs to match the corresponding token pair to the blinded message is signed, and our solution is to use the unified key of the agent to sign. So

Table 3: Computation comparisons with other schemes

Schemes	User	Proxy	Service Provider
priWEL [11]	2N*$T_e{}^G$+4N*$T_m{}^G$	0	N*(N'+1)*$T_e{}^G$+3N*(2N'+3)*$T_m{}^G$
Ours-stage2	T_{BM}+2T_{PE}+2T_{PD}+T_{UM}+T_{SD}	2T_{PD}+3T_{PE}+T_{SE}	0
BlindLocation [18]	T_{BM}+2T_{PE}+T_{PD}+T_{UM}+T_{SD}*M	T_{PD}+T_{PE}+T_p+T_{SE}*M	0
functional pseudonym [16]	6$T_e{}^G$+(M+3)*$T_m{}^G$+2T_{LE}	N*$T_e{}^G$+4N*$T_m{}^G$+N*T_{LD}	0
Ours-stage3	T_{BM}+2T_{PE}+T_{PD}+T_{UM}+T_{SD}*M	2T_{PD}+T_{PE}+T_{SE}*M	0

as the number of agents receiving tasks increases, our solution will be slightly lower than the communication cost in [18].

6.2 Experiment

In this section, we will divide the evaluation into three stages according to the proposed BSLPP scheme. The encryption public key and private key we use here are respectively 128 bytes, the key length used by the blinding function is 128 bytes, and the session key length is 16 bytes. We assume that each identifier ID (including the pseudonym) and HMAC string are 20 bytes; the timestamp size is 3 bytes, and the WiFi fingerprint size is 22 bytes. Broadcast message length is 16 bytes; based on the request information sent by the location service, the size of the response location information and service result information is 20 bytes. According to the knowledge of cryptography, when the length of the plaintext is greater than the key length (bytes) -11, it is necessary to implement fragment encryption in RSA algorithm encryption. When segmentation is not required, the ciphertext length is equal to the key length; otherwise, the ciphertext length is equal to the key length multiplied by the number of slices. We use python language to implement blind signature technology and public and private key encryption process, and use AES-128 scheme to achieve session process protection.

6.2.1 Cost of the Establish Anonymous Collaborative Group

We use the pseudonym calculation time and information transmission time to evaluate the cost of the first stage. It can be seen from Figure 4 that the calculation of pseudonyms does not come from the same user, but different collaborative users calculate their own pseudonyms, so the pseudonym calculation time here will not increase with the increase of users.

Time to measure the pseudonym calculation time that User A needs to wait. It can be seen from Figure 5 that the information interaction between user A and the collaborative user only includes the broadcast information sent by user A and the pseudonym and public key transmitted by the collaborative user. We assume here that user A can only collect 3 to 4 people for each broadcast. If you want to increase collaboration, users must resend the broadcast again. Although the cost of information transmission will increase with the increase in the number of users, it will also ensure the security of the following because of the increase in the number of users.

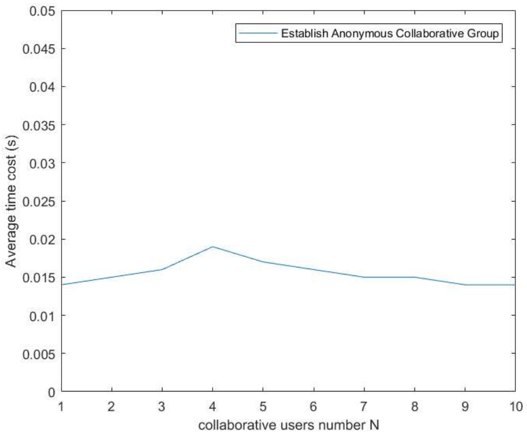


Figure 4: Time spent on encrypting information

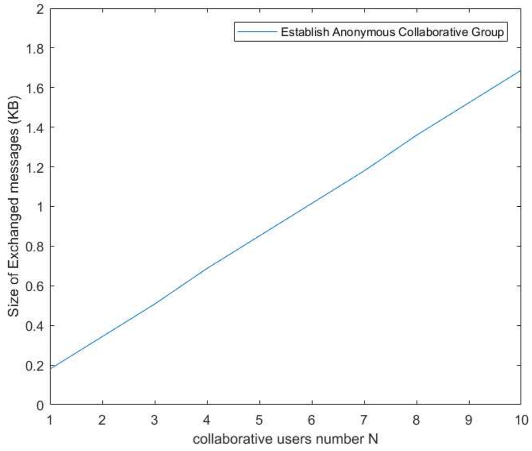


Figure 5: Time spent on exchanging information

6.2.2 Cost of the Protect the Privacy of Location Service

We implemented the priWEL designed in [11] to compare the BSLLP at the stage of protecting the privacy of location services. Based on the comparison of the time spent encrypting the information and the size of the information exchanged, the results are shown in Figure 6 and Figure 7.

In terms of information encryption time, the less infor-

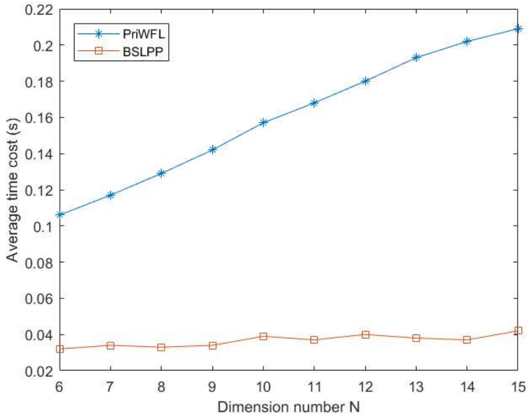


Figure 6: Time spent on encrypting information

mation encryption time, the less time the user spends on location privacy protection. It can be seen from Figure 6 that compared with the priWEL and the BLSSP, it takes less time under the same conditions, and the algorithm is more stable. The increase in the number changes greatly, so it takes less time to encrypt the information, and the responsiveness of the location request is better.

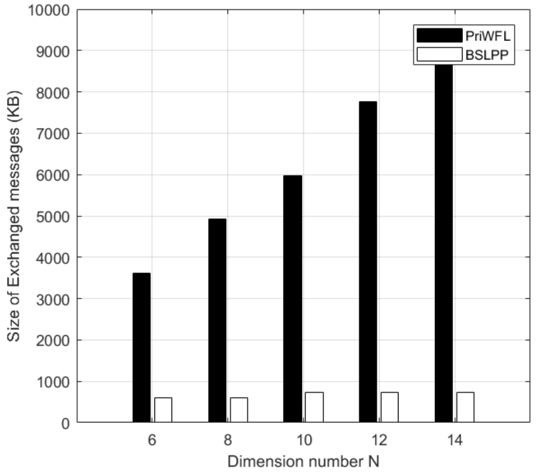


Figure 7: Time spent on exchanging information

In terms of the size of the information exchanged, the smaller the information exchanged, the less time it takes for the location privacy protection process, and the user can get a better experience. As can be seen from Figure 7, under the same conditions of BSLPP and priWEL, as the number of APs increases, the size of the information exchanged by the BSLPP has always been smaller than the priWEL, and will not increase with the number of APs And volatility. In the BSLPP, the hash algorithm we use not only protects the authenticity of the information, but also greatly reduces the bandwidth consumed by the information exchange. At the same time, two methods of the dummy and k-anonymity are used in the solution to ensure the anonymity of the information. The more users communicate with each other at the same time, the higher the anonymity of the information.

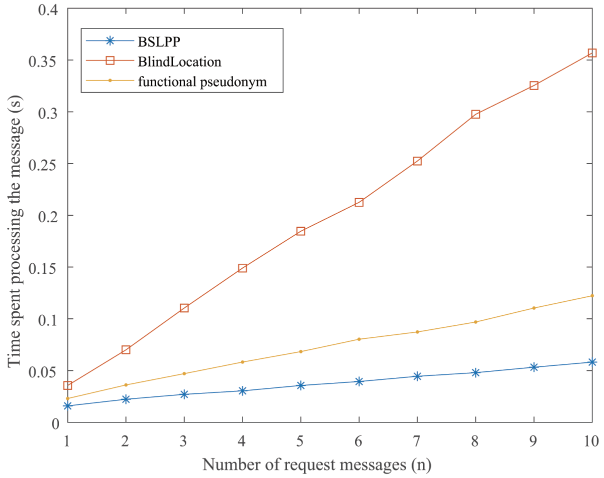


Figure 8: Time spent on location-based service

6.2.3 Cost of the Protect the Privacy of LBS

In the privacy protection stage based on location services, In terms of calculation cost and communication cost, we compare the solution of this paper with the two solutions of BlindLocation [18] and functional pseudonym [16]. In terms of calculation cost, we use CPU running time to represent it, as shown in Figure 8. As far as communication cost is concerned, we measure the size of the exchange message to be displayed, and the specific results are shown in Table 4.

Table 4: Efficency analysis

	Size of Exchanged messages
BSLPP	355 bytes
BlindLocation	227 bytes
functional pseudonym	756 bytes

As can be seen from Table 4, in the privacy protection stage based on location services, we have good performance in terms of encryption and decryption overhead and network overhead, and smartphones can easily implement blind privacy-based location privacy protection solutions. In addition, the scheme provides an acceptable trade-off between privacy and efficiency. We compare this scheme with the existing protocols in Table 5.

As shown in Table 5, in the privacy protection phase of location-based services, our solution has relatively small information exchange, and smartphones can easily implement a location privacy protection solution based on blind signatures. Our scheme does not need any special condition to support privacy, while some of the previous works will do. For example, the remaining solutions cannot achieve the privacy protection of location services and LBSs at the same time. BlindLocation, Obfuscation, and PIR don't protect location privacy in sparsely populated places.

Table 5: Comparison

	BSLPP	BlindLocation	functional pseudonym
Full process protection	Yes	NO	NO
Supporting Anonymity	Yes	Yes	Yes
Missing Quality	NO	NO	NO
Computing Cost	Acceptable	Acceptable	High
Supporting mobile users	Yes	NO	Yes
Untrusted third party server	YES	NO	NO
Supporting sparsely populated areas	Yes	NO	NO

7 Conclusion

This paper considers the issue of mobile user location privacy during the use of location services and location-based queries. We propose a mobile location privacy solution that is compatible with sparsely populated areas. The security analysis of the protocol and the performance analysis and comparison with the existing protocols prove that the scheme has a good performance in terms of user location privacy. The protocol does not need to rely on a trusted or semi-trusted third-party anonymous server to achieve user anonymity, but completes anonymous queries through blind signature technology and guarantees service quality.

In future work, we hope to optimize the algorithm, perform finer-grained verification management for users, and assist query work more efficiently.

Acknowledgments

This article was supported by the National Natural Science Foundation of China Grant (No. 61872230, U1936213, No. 61802248 and No. 61802249), Shanghai Science and Technology Innovation Action Plan (19511103700), Shanghai university young teacher training support program Grant(No. ZZsdl18006). We are very grateful to the reviewers for their valuable comments, and it helpsus to improve the quality of this paper.

References

[1] X. J. Chen and Y. Mu, "Preserving user location privacy for location-based service," in *Green, Pervasive, and Cloud Computing*, pp. 290–300, 2016.

[2] M. L. Damiani and C. Cuijpers, "Privacy challenges in third-party location services," in *IEEE 14th International Conference on Mobile Data Management*, pp. 63–66, June 2013.

[3] Y. Gong, C. Zhang, Y. Fang, and J. Sun, "Protecting location privacy for task allocation in ad hoc mobile cloud computing," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 1, pp. 110–121, 2018.

[4] Q. He, D. P. Wu, and P. Khosla, "The quest for personal control over mobile location privacy," *IEEE Communications Magazine*, vol. 42, no. 5, pp. 130–136, 2004.

[5] M. Hou, H. Zhang, and Y. Wang, "OFC: An approach for protecting location privacy from location provider in location-based services," in *IEEE Third International Conference on Data Science in Cyberspace (DSC'18)*, pp. 917–922, June 2018.

[6] M. S. Hwang, E. F. Cahyadi, H. W. Yang, and C. Y. Yang, "An improvement of the remote authentication scheme for anonymous users using elliptic curves cryptosystem," *IEEE 4th International Conference on Computer and Communications (ICCC'18)*, 2018. DOI: 10.1109/CompComm.2018.8780891.

[7] M. S. Hwang, C. C. Lee, Y. C. Lai, "An untraceable blind signature scheme", *IEICE Transactions on Foundations*, vol. E86-A, no. 7, pp. 1902–1906, July 2003.

[8] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 1683–1687, 2006.

[9] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithmproblem for untraceability," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–841, 2005.

[10] L. Li, R. Lu, and C. Huang, "EPLQ: Efficient privacy-preserving location-based query over outsourced encrypted data," *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 206–218, 2016.

[11] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in wifi fingerprint-based localization," in *IEEE Conference on Computer Communications*, pp. 2337–2345, Apr. 2014.

[12] J. Liao, Y. H. Qi, P. W. Huang, M. T. Rong, and S. H. Li, "Protection of mobile location privacy by using blind signature," *Journal of Zhejiang University Science*, vol. 7A, no. 6, pp. 984–989, 2006.

[13] G. Natesan and J. G. Liu, "An adaptive learning model for k-anonymity location privacy protection," in *IEEE 39th Annual Computer Software and Applications Conference*, 2015. DOI: 10.1109/COMPSAC.2015.281.

[14] T. Peng, Q. Liu, and G. Wang, "Enhanced location privacy preserving scheme in location-based services," *IEEE Systems Journal*, vol. 11, no. 1, pp. 219–230, 2017.

[15] J. H. Qin and H. L. Luo, "User privacy disclosure and protection in location-based services (in chinese)," *Computer Programming Skills and Maintenance*, vol. 08, no. 113–114, 2015.

[16] J. Son, D. Kim, M. Z. A. Bhuiyan, R. Tashakkori, J. Seo, and D. H. Lee, "Privacy enhanced location sharing for mobile online social networks," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 279–290, 2018.

[17] Q. G. Song and J. Wang, "Wifi location fingerprinting positioning method of privacy protection technology research and implementation," Technical Report, June 2017.

[18] M. A. Talouki, A. B. Dastjerdi, and N. Movahedinia, "Blindlocation: Supporting user location privacy using blind signature," in *The 7th International Conference on Computer and Knowledge Engineering (ICCKE'17)*, pp. 53–59, Oct. 2017.

[19] L. Y. Wang, D. Q. Yang, and X. Han, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proceedings of the 26th International Conference on World Wide Web*, pp. 627–636, 2017.

[20] Y. H. Wang, H. L. Zhang, and X. Z. Yu, "KAP: Location privacy-preserving approach in location services (in chinese)," *Journal of Communications*, vol. 35, no. 11, pp. 182–190, 2014.

[21] S. S. Wu, J. B. Xiong, G. H. Ye, and Z. Q. Yao, "Research on location privacy protection based on fake location in mobile internet environment (in chinese)," *Information Network Security*, vol. 10, no. 54–59, 2016.

[22] R. Y. Yu, Z. H. Bai, L. Y. Yang, P. F. Wang, and Y. H. Liu, "A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks," *IEEE Access*, vol. 4, pp. 6515–6527, 2017.

[23] A. Y. Ye, Y. C. Li, and L. Xu, "A novel location privacy-preserving scheme based on l-queries for continuous LBS," *Computer Communications*, vol. 98, no. 1–10, 2016.

[24] X. J. Zhang, X. L. Gui, and Z. D. Wu, "A survey of location service privacy protection (in chinese)," *Journal of Software*, vol. 26, no. 9, pp. 2373–2395, 2015.

[25] D. P. Zhao, J. S. Ma, X. L. Wang, and X. X. Tian, "Personalized location anonymity - A kernel density estimation approach," in *Web-Age Information Management*, pp. 52–64, June 2016.

[26] L. J. Zheng, H. H. Yue, L. H. Zhang, and X. Pan, "A new location privacy protection algorithm," *IEEE International Conference on Computational Science and Engineering and IEEE International Conference on Embedded and Ubiquitous Computing*, 2017. DOI: 10.1109/CSE-EUC.2017.253.

[27] Y. J. Zhu, "Analysis and assessment of privacy disclosure risks in location-based services (in chinese)," *Guizhou University*, vol. 03, no. 1–73, 2016.

[28] H. Zhu, F. Liu, and H. Li, "Efficient and privacy-preserving polygons spatial query framework for location-based services," *IEEE Internet Things*, vol. 4, no. 2, pp. 536–545, 2017.

Biography

Xin Xu Graduate. College of Computer Science and Technology in Shanghai University of Electric Power. He research interests mainly focus on the security and privacy protection for the location.

Mi Wen(M'10) Received the M.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2005, and the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, in 2008, both in computer science. She is currently an Associated Professor of the College of Computer Science and Technology with Shanghai University of Electric Power, Shanghai, China. From May 2012 to May 2013, she was a Visiting Scholar at the University of Waterloo, Waterloo, ON, Canada. Her research interests include privacy preserving in wireless sensor network, smart grid, etc. Dr. Wen serves as an Associate Editor of Peer-to-Peer Networking and Applications (Springer). She acts as the TPC Member of some flagship conferences such as the IEEE INFOCOM, the IEEE ICC, and the IEEE GLOEBECOM.

Liangliang Wang Received his Ph.D. degree from Shanghai Jiao Tong University, in 2016. Currently, he is a assistant professor in College of Computer Science and Technology, Shanghai University of Electric Power. His research interests include information security and smart grid, etc.