Location-Sharing Protocol for Privacy Protection in Mobile Online Social Networks

Ou Ruan
Hubei University of Technology https://orcid.org/0000-0001-8189-3258
Lixiao Zhang
Hubei University of Technology
Yuanyuan Zhang (circle0519@hotmail.com)
University of Technology

Research

Keywords: Location privacy, Location sharing, Mobile online social networks, Smart cities

Posted Date: December 31st, 2020

DOI: https://doi.org/10.21203/rs.3.rs-135686/v1

RESEARCH

Location-Sharing Protocol for Privacy Protection in Mobile Online Social Networks

Ou Ruan, Lixiao Zhang and Yuanyuan Zhang*

*Correspondence:
circle0519@hotmail.com
School of Computers, Hubei University of Technology, No.28, Nanli Road, Hong-shan District, 430068 Wuhan, China
Full list of author information is available at the end of the article

Abstract

Location-based services are becoming more and more popular in mobile online social networks(mOSNs) for smart cities, but users' privacy also has aroused wide concern, such as locations, friend sets and other private information. At present, many location sharing protocols in mOSNs have been proposed, but these protocols are inefficient and ignore some security risks. In this paper, we propose a new location sharing protocol, which solves these two issues by using symmetric encryption and asymmetric encryption properly. We adopt the following methods to reduce the communication and computation costs: only setting up one location server; connecting social network server and location server directly instead of through celluar towers; avoiding broadcast encryption. We introduce dummy identities to protect users' identity privacy, and prevent location server from inferring users' activity tracks by updating dummy identities in time. The details of security and performance analysis with the related protocols show that our protocol enjoys two advantages: (1) it's more efficient than the related protocols, which greatly reduces the computation and communication costs; (2) it satisfies all security goals, however, most previous protocols only meet some security goals.

Keywords:
Location privacy, Location sharing, Mobile online social networks, Smart cities.

1 Introduction

Smart city [1], [2], [3] is an agglomeration of urban society that employs intelligent technologies to improve how people live, work, commute and share information. A key aspect of a smart city is mobile online social networks (mOSNs) [4], [5], [6], [7], [8] that are popular mainstream platforms for information and content sharing among people. Location sharing is an important component of mOSNs and also has attracted much attention recently. No matter where a person is, nearby people can be matched by applications such as WeChat, Facebook and Twitter [9], which change traditional social ways and help people broaden their circle of friends [10].

With the increasing popularity of location-based services, the risk of leakage of users' privacy also increases. According to users' location information, users' activity track can be obtained by criminals. Furthermore, users' private information such as health condition, home address, work unit can be inferred [11]. This threat becomes even more serious when it comes to mOSNs, in which users' physical locations are being correlated with their profiles [12, 13]. Without a guarantee of privacy, users may be hesitant to share locations through mOSNs [14]. Therefore, how to protect users' privacy is one of main challenges in mOSNs. So many studies have been proposed to protect users' privacy and they are mainly divided into the following two categories:

(1) *K-anonymity*. The typical method *K-anonymity* [15], [16] is used to obscure the real location by generating $(k-1)$ virtual locations. That is to say, k positions are generated, including one real position and $(k-1)$ dummy positions to prevent attackers from identifying the real position. However, firstly, some protocols set up celluar towers, which are used to connect social newtwork server and location server, and will increase communication costs of the whole system. Secondly, in some protocols, query results contain the real identity, which leaks the identity privacy. Thirdly, some protocols don't verify the identity of sender, that is to say, these protocols don't conduct identity authentication.

(2) *Dummy identity*. The main idea of the dummy identity method [17], [18] is to only share location but hide identity. The method anonymizes users' identities by adopting pseudonyms. However, some protocols set up multiple location servers and adopt broadcast encryption, which increases communication and computation costs. On the other hand, in some protocols, location servers can infer users' activity tracks and further learn sensitive information such as health state.

From the above analysis, these methods suffer two constraints: (1) they are inefficient and have high communication and computation costs. (2) they ignore some security goals. In this paper, we propose a new location sharing protocol, which solves two issues by using symmetric encryption and asymmetric encryption properly. Firstly, in our protocol, only one location server is set up, broadcast encryption isn't needed, and social network server and location server are connected directly instead of connecting through celluar towers, thus we greatly reduce computation and communication costs. Secondly, inquirers only get dummy identities rather than real identities, which protects users' identity privacy. Thirdly, we prevent location server from inferring users' activity track by updating dummy identities in time. Fourth, we conduct identity authentication to prevent impersonation attacks.

Compared with the related articles, our advantages are as follows:

- Our protocol greatly reduces computation and communication costs. In our protocol, firstly, only one location server rather than multiply location servers is set up to reduce communication and computation costs. secondly, we apply symmetric encryption instead of broadcast encryption to reduce communication and computation costs. Thirdly, cellular towers aren't set up to reduce communication costs.
- Our protocol satisfies all security goals, however, most previous protocols only meet some security goals.

This paper is organized as follows. The related works are given in Section 2. In Section 3, the preliminary is provided. In Section 4, our new method is proposed. Result and discussion is presented in Section 5. Conclusion is described in Section 6.

2 Related Works

According to the underlying cryptographic techniques, there are two common methods: *K-anonymity*, *Dummy identity*.

K-anonymity. The typical method *K-anonymity* was first proposed by Sweeney *et al.* [15] in 2002 and then, Gruteser *et al.* [16] used it for location privacy protection, Kido *et al.* [17] extended *K-anonymity* and introduced the concept

of virtual location. But the method *K-anonymity* has an obvious disadvantage: it incurs great communication and computation costs.

In 2004, a location sharing protocol [19] which can hide users' positions in sensitive areas by location updation was proposed. But users may be traced by location servers. In order to solve the problem, an improved model [20] called *CacheCloak* was proposed by Meyerowitz *et al.*. *CacheCloak* is a system that makes location data anonymous in real time. In *CacheCloak*, a trusted anonymizing server generates mobility predictions from historical data and submits predicted paths simultaneously to location server. Each new predicted path is made to intersect with other users' paths, ensuring that no individual user's path can be reliably tracked over time. That is to say, *CacheCloak* prevents untrusted location servers tracking users while providing highly accurate realtime location updates.

In 2015, *BMobishare* model [21] which employs Bloom Filter to mask sensitive data was proposed by Shen *et al.*. It employs Bloom Filter, thus a malicious user can not obtain unauthorized privacy information. But it ignores identity privacy and identity authentication. Identity privacy: query results contain the real identities which leak the identity privacy. Identity authentication: if a server doesn't verify received information, an attacker may send a location message to the server by pretending the identity of a legitimate user. In 2019, Chen *et al.* presented a new model [22] to protect identity privacy and conduct identity authentication.

Dummy identity. The typical method *Dummy identity* was first proposed by Cox *et al.* [18] in 2007, called *SmokeScreen* model, where a user ID_i sets up his access control policies df_{ID_i} for friends and ds_{ID_i} for strangers. Friends or strangers can obtain users' locations if they satisfy the access control policies. However, in *SmokeScreen* model, there is only one server used to store personal information such as social network relation and location, if a malicious user colludes with the server, the identity information and the corresponding location information will be obtained by the malicious user. In 2012, Wei *et al.* [23] proposed *Mobishare* model to solve this problem. The model sets two servers: location server and social network server. Location server is used to store location data and social network server is used to store personal information such as social relation. That is to say, neither the social network server nor the location server has a complete information including the users' identities and locations. So users' privacy are protected even if location server or social network server colludes with malicious users. But users' social relations can be infered by location server. In 2013, Li *et al.* [24] proposed *Mobishare+* model, which can be seen as an improved mechanism based on Mobishare model. It employs dummy queries and private set intersection protocol to prevent the social network server and location server from learning individual information from each other. In 2013, Liu *et al.* [25] proposed *N-Mobishare* model based on *Mobishare* model. Compared with *Mobishare* model and *Mobishare+* model, celluar towers aren't set up in *N-Mobishare* that is used to connect social network server and location server, thus *N-Mobishare* reduces communication costs. In 2014, an improved model [26] of *N-Mobishare* which can prevent location server from inferring social relation of users was proposed. Social network server generates a set containing dummy identities of an inquirer's all friends and adds some randomly dummy identities to further anonymize the inquirer's real social relation. But the model adopts broadcast

encryption which requires user to dynamically change his sharing decryption key when a friend is added or revoked, which will lead to great communication and computation costs.

In 2017, a new framework and a new query algorithm (UDPLS) [27] were proposed to protect users' location privacy on social network server and user's social network privacy on location server. Users can share location with specified-friends instead of all friends. Li *et al.* [28] proposed the structure of multiple location servers. When a user queries locations of friends, the social relation of the user will be randomly divided into multiple subsets by the social network server, and these subsets will be sent to different location servers. However, when a user updates his location, the location is encrypted by the secret keys of multiple location servers and sent to every location server, thus it results in great communication and computation costs. In addition, although the location server only stores users' anonymous identities, their activity tracks also can be inferred. In 2020, Xu *et al.* [29] proposed the structure of multiple location servers to protect the activity track privacy. However, because of using multiple location servers, the protocol had a common shortcoming: higher communication and computation costs.

3 Preliminaries

3.1 System Model

We illustrate system architecture in Figure 1, where are three entities.

Users. A user is an entity who locates the current location through his mobile phone. He can share his current location with the nearby friends or strangers, and can also query the locations of friends or strangers in his self-defined range.

Online social network server. This entity, denoted by S_{OSN}, provides online social services and manages every user's personal materials such as his friends set, friend's access control policy df_{ID_i} and stranger's access control policy ds_{ID_i}. In S_{OSN}, each user has a corresponding dummy identity.

Location Server. This entity, represented as S_{LS}, manages users' dummy identities and locations, and returns the location information to the queriers.

3.2 Threat Model

Users may be dishonest and try to get all the location information which meet their needs, but some of the location information are beyond users' right.

S_{OSN} and S_{LS} are both considered as "honest-but-curious", S_{OSN} may attempt to get the location information which should be managed by S_{LS}, and S_{LS} may try to gain the social relation which is stored in S_{OSN}.

In our security model, we don't allow users to collude with S_{OSN} or S_{LS}. On the other hand, we don't allow S_{OSN} and S_{LS} to collude and obtain information of each other.

3.3 Security Goals

In our model, the security goals have the following six aspects:

- Authorized access. A user's location can't be accessed by friends or strangers who do not conform to the user's access control policies df_{ID_i} or ds_{ID_i}.

- Identity privacy. Users can only get friends' or strangers' dummy identities as query results, and they can't collude with S_{OSN} to get the real identities of friends or strangers.
- Social relation privacy. S_{LS} should be prevented from obtaining users' personal materials such as the social relation.
- Location privacy. S_{OSN} should be prevented from obtaining users' locations.
- Activity track privacy. S_{LS} should be prevented from inferring users' activity tracks.
- Identity authentication. Some measures should be taken to prevent users' identities from being impersonated.

3.4 Notation

We summarize main notations in Table 1

Table 1: Table of notation

Notation	Description
ID_i	User i's social network identifier
FID_i	dummy identity of user ID_i
S_{LS}	Location server
S_{OSN}	Social network server
(x_i,y_i)	User ID_i's real location
df_{ID_i}	User ID_i's friend-case threshold distance
ds_{ID_i}	User ID_i's stranger-case threshold distance
G	A social network graph stored in S_{OSN}
I	User's query scope in the stage of friends' or strangers' location query
(pk_{ID_i}, sk_{ID_i})	User ID_i's public key and secret key pair
(pk_{osn}, sk_{osn})	The public key and secret key pair of S_{OSN}
(pk_{LS}, sk_{LS})	Location server's public key and secret key pair
dist((x_1, y_1),(x_2, y_2))	The function calculates the distance between (x_1, y_1) and (x_2, y_2)
min(x,y)	The function that computes the minimum of x and y

4 Our methods

4.1 A New Location Sharing Protocol for Privacy Protection

The details of our location-sharing protocol are as follows:

a. **System Initialization.**

1). A user ID_i generates his public key and secret key pair (pk_{ID_i}, sk_{ID_i}) and defines his access control policy df_{ID_i} and ds_{ID_i}. In the friends' location query phase, df_{ID_i} refers to the condition that other users must satisfy if they want to access user ID_i's location. Similarly, ds_{ID_i} is applied to the strangers' location query stage. Personal data $(ID_i, pk_{ID_i}, df_{ID_i}, ds_{ID_i})$ is stored at S_{OSN}.

2). S_{OSN} generates his public key and secret key pair (pk_{osn}, sk_{osn}) and stores a social network graph G which involves all users' social relation.

3). S_{LS} generates his public key and secret key pair (pk_{LS}, sk_{LS}).

b. **User Registration.**The details of registration are descriped in Fig.2

1). User ID_i generates a signature with his secret key σ_{ID_i}=$Sig_{sk_{ID_i}}(ID_i, ts)$, where ts is a timestamp, and encrypts authentication information $(ID_i, ts, \sigma_{ID_i})$ and his current location *(x,y)* to generate $C_{ID_i} = E_{pk_{osn}}(ID_i, ts, \sigma_{ID_i})$, $c = E_{pk_{LS}}(x, y)$, then sends (C_{ID_i}, c) to S_{OSN}.

2). Upon receiving (C_{ID_i}, c), S_{OSN} decrypts C_{ID_i} and gains $(ID_i, ts, \sigma_{ID_i})$ and verifies whether the digital signature σ_{ID_i} is correct to ensure the location information belongs to ID_i. If the authentication passes, S_{OSN} randomly generates a dummy identity FID_i and stores the record $(ID_i, FID_i, df_{ID_i}, ds_{ID_i}, pk_{ID_i})$ at S_{OSN}, then sends (FID_i, c) to S_{LS}.

3). S_{LS} decryptes c to acquire location information *(x,y)* and stores the record $(FID_i, (x, y))$ at S_{LS}.

c. **Location Update.**The details of location update are described in Fig.3

1). User ID_i generates the authentication information C_{ID_i} and cipertext c of the current newest location (x, y) and sends them to S_{OSN}, C_{ID_i}=$E_{pk_{osn}}(ID_i, ts, \sigma_{ID_i})$, c=$E_{pk_{LS}}(x, y)$.

2). Upon receiving the information, S_{OSN} decrypts C_{ID_i} and verifies whether the digital signature σ_{ID_i} is correct, If the authentication passes, S_{OSN} randomly generates a dummy identity FID_i and replaces the previous FID_i. That is to say, each user has a unique dummy identity. Then the latest dummy identity is updated in the personal information $(ID_i, FID_i, df_{ID_i}, ds_{ID_i}, pk_{ID_i})$ at S_{OSN}. S_{OSN} signs the latest dummy identity as well as the timestamp ts, it can be expressed as σ_{OSN}=$Sig_{sk_{osn}}(FID_i, ts)$. S_{OSN} sends $((FID_i, ts), \sigma_{OSN}, c)$ to S_{LS}.

3). Upon receiving $((FID_i, ts), \sigma_{OSN}, c)$, S_{LS} verifies whether σ_{OSN} is correct, if the verification passes, the latest FID_i and *(x,y)* are stored at S_{LS}.

d. **Friends' Location Query.**The details of friends' location query are described in Fig.4. At this stage the inquirers can query the location of friends according to their own needs. $'l'$ can be understood as the distance threshold formulated by a inquirer.

1). Inquirer ID_i generates a one-time symmetric key k and encrypts k and his own current location information (x, y) to generate c, c=$E_{pk_{LS}}(x, y, k)$. The inquirer also encrypts the query condition $(ID_i, 'F', l)$ to generate C_{ID_i}=$E_{pk_{osn}}(ID_i, 'F', l)$, where *'F'* denotes the symbol of friend query. The inquirer sends (C_{ID_i}, c) to S_{OSN}.

2). Upon receiving the information, S_{OSN} decrypts C_{ID_i} and gets $(ID_i, 'F', l)$. S_{OSN} matches inquirer's friends set and matches each friend's (ID_j, FID_j, df_{ID_j}). Then S_{OSN} calculates each friend's dm_{ID_j} which is expressed as dm_{ID_j}=$min(df_{ID_j}, l)$, and matches (FID_j, dm_{ID_j}) of all friends to form the set S. Suppose the number of the inquirer's friends is m, $S = ((FID_1, dm_{ID_1}), .., (FID_m, dm_{ID_m}))$. Then S_{OSN} encrypts the set S to generate $C_{LS} = E_{pk_{LS}}(S)$ and sends (C_{LS}, c) to S_{LS}.

3). Upon receiving the information, S_{LS} decrypts c and C_{LS} and matches the corresponding position (x_j, y_j) and checks which member can meet the condition $dist((x, y), (x_j, y_j)) <= dm_{ID_j}$. If a member FID_j meets the condition, S_{LS} encrypts the location information c_{ID_j}=$E_k(FID_j, (x_j.y_j))$. Suppose there are p qualified members whose position information constitutes the set M. M is represented as $M = (c_{ID_1}, c_{ID_2}, c_{ID_3}, ..., c_{ID_p})$. S_{LS} sends the set M to S_{OSN} and S_{OSN} sends M to the inquirer.

4). The inquirer decrypts and gets all of the location information $(FID_j, (x_j, y_j))$ in the set M.

e. **Strangers' Location Query.**The details of strangers' location query are described in Fig 5. At this stage the inquirers can query the location of strangers according to their own needs. $'l'$ can be understood as the distance threshold formulated by a inquirer.

1). Inquirer ID_i generates a one-time symmetric key k and encrypts k and his own current location information (x, y) to generate c, c=$E_{pk_{LS}}(x, y, k)$. The inquirer also encrypts the query condition $(ID_i,' S', l)$ to generate C_{ID_i}=$E_{pk_{osn}}(ID_i,' S', l)$, *'S'* denotes the symbol of stranger query. The inquirer sends (C_{ID_i}, c) to S_{OSN}.

2). Upon receiving the information, S_{OSN} decrypts C_{ID_i} and gets $(ID_i,' S', l)$. S_{OSN} matches inquirer's strangers set and matches each stranger's (ID_j, FID_j, ds_{ID_j}). Then S_{OSN} calculates each stranger's dm_{ID_j} which is expressed as $dm_{ID_j} = min(ds_{ID_j}, l)$ and matches (FID_j, dm_{ID_j}) of all strangers form the set S. Suppose the number of the inquirer's strangers is m, then the set S can be expressed as $S = ((FID_1, dm_{ID_1})..(FID_m, dm_{ID_m}))$. Then S_{OSN} encrypts the set S to generate $C_{LS} = E_{pk_{LS}}(S)$ and sends (C_{LS}, c) to S_{LS}.

3). Upon receiving the information, S_{LS} decrypts c and C_{LS} and matches the corresponding position (x_j, y_j) and checks which member can meet the condition $dist((x, y), (x_j, y_j)) <= dm_{ID_j}$. If a member FID_j meets the condition, S_{LS} encrypts the location $C_{ID_j} = E_k(FID_j, (x_j.y_j))$. Suppose there are p qualified members whose position information constitutes the set M. M is represented as M=$(c_{ID_1}, c_{ID_2}, c_{ID_3}, ..., c_{ID_p})$. S_{LS} sends the set M to S_{OSN} and S_{OSN} sends M to the inquirer.

4). The inquirer decrypts and gets all of the location information $(FID_j, (x_j, y_j))$ in the set M.

4.2 Security Analysis

In this section, we gave the analysis of security as following:

1). Authorized access. Every user defines his access conditions df_{ID_i} which is used to friends' location query and ds_{ID_i} which is used to strangers' location query. Only when a querier satisfies a user's df_{ID_i} or ds_{ID_i}, he can obtain the user's location information. Otherwise, the user's location information will be protected and can't learned by the querier.

2). Identity privacy. When users query friends' or strangers' locations, S_{OSN} matches and sends all friends' dummy identities rather than real identities to the S_{LS}, then S_{LS} sends them to inquirers. so, in the process of query, inquirers can't get friends' or strangers' real identities, so that identity privacy is protected.

3). Social relation privacy. If a user is constantly updating his or her locations, *FID* is constantly changed. Then when different inquirers inqury a common friend's location, they are matched different dummy identities in S_{LS}. S_{LS} will assume that different users are being queried, thus records in S_{LS} are not linked to the common friend, which prevents the user's friends relation from being acquired by S_{LS}.

4). Location privacy. In the location updation stage and location query stage, location information is sent to S_{OSN} in the form of ciphertext, which means that the location of users are avoided to be obtained by S_{OSN}.
5). Activity track privacy. When a user updates his location, S_{OSN} assigns different *FID* and S_{LS} stores the newest *FID* and location. In other word, S_{LS} stores several records which belong to the same user, but S_{LS} believes every record belongs to different users due to the different *FID* and doesn't connect the records with the same user and can't infer users' activity tracks.
6). Identity authentication. When S_{OSN} receives a user's location, it verifies the user's identity. So the user's identity will not be impersonated.

5 Results and discussion

5.1 Implementation

We ran our experiments for mobile users in a Xiaomi smartphone with Android operation system. The location server is simulated with the Intel(R) Core(TM)i7-8750H 2.20-GHz CPU. The social network server is simulated with Alibaba Cloud in Ubuntu18.04 with linux 4.4.0.59. Our privacy-preserving location-sharing system was implemented using the Bouncycastle library for the cryptographic operations. The following cryptography tools are included in our implementation: SM2 encrypt/decrypt algorithm, SM2 signature/verify algorithm, SM3 hash algorithm and AES encrypt/decrypt algorithm. To get the user's location information, we use Amap API to get the real geographical position. We give the running times of two main stages in our system in Table 2.

5.2 Discussion

A detailed analysis with other related protocols is given in Table 3 and 4. We evaluate the performance in terms of two aspects: communication and computation complexity; security goals.

1). **Communication and Computation complexity.**
   (a) Communication complexity. The communication cost of our protocol is $3\lambda+\mu$ in the location update phase and is $(2p+4)\mu$ in the location query phase. Thus, the overall communication complexity of our protocol is $O(1)$, which is constant. Both of [28] and [29] are $O(n^2)$, where n is the number of location sever. Finally the protocols in [21], [30] and [22] are $O(k)$, where k is virtual locations.
   (b) Computation complexity. We evaluate the computation cost by counting the number of encryption/decryption and sinature/verify operation, as their cost dominates that of other operations in the protocol. More specifically, the location update phase includes two encryption and decryption operations and two verification operations, while the location query phase includes $3+p$ encryption and decryption operations. Thus, the computation complexity is $O(1)$, which is constant. The computation complexity of the protocols [28] and [29] are $O(n)$, while in protocols [21], [30] and [22] are $O(k)$, where k is virtual locations.
2). **Security Goals**. We can see that our protocol meets all security goals, but protocols [30], [21] and [28] only meet part of security goals in Table 4. Our protocol and [22] only need one location server and get rid of cellular towers

and broadcast encryption. *Cellular towers* in [21] and [30] that are used to connect social network server to location server and thus increase the communication costs. [28] and [29] set up *multiple location servers*, which cause great communication and computation costs. *Broadcast encryption* [28] leads to great communication and computation costs. Since the ciphertext is encrypted with the key shared with the current authorized users, if a user joins or exits, in order to ensure the security of the broadcast, the keys of current authorized users must be updated, which leads to great communication and computation costs. *Identity privacy*: in the location query stage of [30], [21], the query results contain users' real identities, thus the identity privacy isn't considered. In our protocol, inquirers get dummy identities rather than real identities, thus users' identity privacy are preserved. *Activity track privacy*: in [28], location server is used to store location information, but location server can infer the activity track and further learn sensitive information such as interest and health state, which will pose a great security threat to users. In our protocol, we protect activity track privacy by updating user's dummy identities. *Identity authentication*: in the communication process of [30], [21] which evade the identity authentication, an attacker may send a location message to servers by pretending a legitimate user's identity, if the servers do not verify the received information, they will store the wrong location message. In our protocol, socail network service will conduct identity authentication to avoid this security problem.

Table 2: The running time(ms) of the two stages

Stage \ Entity	user	social network server	location server
Location Update	453	130	34
Location Query	150	75	20

Table 3: Comparison of security goals with other related protocols

Protocol	Cellular Towers	Broadcast Encryption	The Number of S_{LS}	Authorized Access	Identity Privacy	Social Relation Privacy	Location Privacy	Activity Track Privacy	Identity authentication
Nan Shen 2015 [21]	Yes	No	1	Yes	No	Yes	Yes	Yes	No
Jin Li 2017 [28]	No	Yes	n	Yes	Yes	Yes	Yes	No	Yes
Xi Xiao 2018 [30]	Yes	No	1	Yes	No	Yes	Yes	Yes	No
Juan Chen 2019 [22]	No	No	1	Yes	Yes	Yes	Yes	Yes	Yes
Chang Xu 2020 [29]	No	No	n	Yes	Yes	Yes	Yes	Yes	Yes
Our Protocol	No	No	1	Yes	Yes	Yes	Yes	Yes	Yes

Table 4: Comparison of computation and communication costs with related protocols

Protocol	Communication costs		Computation costs	
	Location updation	Location query	Location updation	Location query
Nan Shen 2015 [21]	(k+1)λ	(3p+3)λ	k.Enc-asym + k.Dec-asym	p.Enc-sym +Enc-asym +p.Dec-sym +Dec-asym
Jin Li 2017 [28]	(n+n^2)λ+μ	(n+n^2+2p)λ	n.Enc-asym + n.Dec-asym + Sig+ Ver	(n+p).Enc-asym + (n+p).Dec-asym
Xi Xiao 2018 [30]	(k+1)λ	(2p+1)λ	k.Enc-asym +k.Dec-asym	(p+1).Enc-asym + (p+1).Dec-asym
Juan Chen 2019 [22]	(k+1)λ + 2μ	2pλ + 4μ	k.Enc-asym +k.Dec-asym +Sig +Ver	p.Enc-asym + p.Dec-asym + Sig + Ver
Chang Xu 2020 [29]	(2n^2+2n)λ + μ	(n^2+t+2p+n)λ	2n.Enc-asym + 2n.Dec-asym +Sig +Ver	(t+n+p)Enc-asym + (t+p+n)Dec-asym
Our Protocol	3λ + μ	(2p+4)λ	2.Enc-asym + 2.Dec-asym +2.Sig+2.Ver	3.Enc-asym + p.Enc-sym+3.Dec-asym +p.Dec-sym

λ: the length of elements calculated by elliptic curve encryption operation
μ: the length of elements calculated by elliptic curve signature operation
p: In the location query stage of friends and strangers, the number of members meeting the requirements of the inquirer
n: the number of location services
Enc-sym: a symmetric encryption operation
Enc-asym: an asymmetric encryption operation
Dec-sym: a symmetric decryption operation
Dec-asym: an asymmetric decryption operation
Sig: a elliptic curve signature operation
Ver: an operation to verify the validity of an elliptic curve signature
k: one real location and (k-1) virtual locations generated by k anonymous
t: the number of friends assigned to each location server

6 Conclusion

In this paper, we proposed an efficient location sharing protocol to protect privacy in mOSNs for smart cities, which not only supported location sharing among friends and strangers, but also protected users' privacy. Although our protocol was more efficient than other related protocols and achieved all security goals, there is still storage pressure that need to be improved. In the future, we can further improve our protocol according to the following method: during the location update phase, we can reduce storage pressure on the location server by regularly deleting invalid records in the location server.

Abbreviations
S_{OSN}: Social network server; S_{LS}: Location server

Acknowledgements
Not applicable

Authors' contributions
The authors have contributed jointly to all parts on the preparation of this manuscript, and all authors read and approved the final manuscript.

Funding
This work is supported by the National Natural Science Foundation of China under grants 61701173, 61672010 and 61702168, the fund of Hubei Key Laboratory of Transportation Internet of Things (WHUTIOT-2017B001), and the Ph.D. research startup foundation of Hubei University of Technology (BSQD2015028).

Availability of data and materials
Not applicable

Competing interests
The authors declare that they have no competing interests.

Author details
School of Computers, Hubei University of Technology, No.28, Nanli Road, Hong-shan District, 430068 Wuhan, China.

References

1. Y. Chen, X. Zou, K. Li, X. Yang, C. Chen, Multiple local 3D CNNs for region-based prediction in smart cities. Information Sciences. 542, 476-491(2021). https://doi.org/10.1016/j.ins.2020.06.026
2. G. Premsankar, B. Ghaddar, M. Slabicki and M. D. Francesco, Optimal Configuration of LoRa Networks in Smart Cities. in: IEEE Transactions on Industrial Informatics. (2020), pp. 7243-7254. https://doi.org/10.1109/TII.2020.2967123
3. Sandoval, R.M., Garcia-Sanchez, A.Garcia-Haro, J, Performance optimization of LoRa nodes for the future smart city/industry. J Wireless Com Network, 2019(1), 200(2019). https://doi.org/10.1186/s13638-019-1522-1
4. J. Liu, L. Fu, X. Wang, F. Tang and G. Chen, Joint Recommendations in Multilayer Mobile Social Networks. in: IEEE Transactions on Mobile Computing. (2020), pp. 2358-2373. https://doi.org/10.1109/TMC.2019.2923665.

5. A. M. Vegni, C. Souza, V. Loscrí , E. Hernández-Orallo and P. Manzoni, Data Transmissions Using Hub Nodes in Vehicular Social Networks. in: IEEE Transactions on Mobile Computing. (2020), pp. 1570-1585. https://doi.org/10.1109/TMC.2019.2928803.
6. Sun, Z., Kou, H. Huang, W, Privacy-aware friend finding in social network based on thumbs-up data. J Wireless Com Network. 2019(1), 211(2019). https://doi.org/10.1186/s13638-019-1538-6
7. C. Yan, Z. Ni, B. Cao, R. Lu, S. Wu, Q. Zhang, Umbrella: user demand privacy preserving framework based on association rules and differential privacy in social networks. Sci China Inf Sci.62(3),39106(2018). http://dx.doi.org/10.1007/s11432-018-9483-x
8. X. Ju, K. G. Shin, Location privacy protection for smartphone users using quadtree entropy maps. Journal of Information Privacy and Security. 11(2), 62–79(2015). http://dx.doi.org/10.1080/15536548.2015.1045372
9. H. T. Dinh, C. Lee, D. Niyato, P. Wang, A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing. 13(18), 1587–1611(2013). http://dx.doi.org/10.1002/wcm.1203
10. N. Li, G. Chen, Sharing location in online social networks. IEEE network. 24(5), 20–25(2010). http://dx.doi.org/10.1109/MNET.2010.5578914
11. Y. Sun, M. Chen, L. Hu, Y. Qian, M. M. Hassan, Asa: Against statistical attacks for privacy-aware users in location based service. Future Generation Computer Systems. 70, 48–58(2017). https://doi.org/10.1016/j.future.2016.06.017
12. L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, M. Chalmers, From awareness to repartee: sharing location within social groups. in Proceedings of the SIGCHI conference on human factors in computing systems. (2008), pp. 497–506. https://doi.org/10.1145/1357054.1357134
13. E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, N. Sadeh, Empirical models of privacy in location sharing. in: Proceedings of the 12th ACM international conference on Ubiquitous computing. (2010), pp. 129–138. https://doi.org/1145/1864349.1864364
14. L. Barkhuus, A. K. Dey, Location-based services for mobile telephony: a study of users' privacy concerns. in: Human-computer Interaction Interact 03: Ifip Tc13 International Conference on Human-computer Interaction. (2003), pp. 702–712.
15. L. Sweeney, k-anonymity: A model for protecting privacy. International Journal of Uncertainty Fuzziness and Knowledge-Based Systems. 10(05), 557–570(2002). https://doi.org/10.1142/S0218488502001648
16. M. Gruteser, D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking. in: Proceedings of the 1st international conference on Mobile systems, applications and services. (2003), pp. 31–42.
17. H. Kido, Y. Yanagisawa, T. Satoh, Protection of location privacy using dummies for location-based services. in: 21st International Conference on Data Engineering Workshops (ICDEW'05). (2005), pp. 1248–1248. https://doi.org/10.1109/ICDE.2005.269.
18. L. P. Cox, A. Dalton, V. Marupadi, Smokescreen: flexible privacy controls for presence-sharing. in: Proceedings of the 5th international conference on Mobile systems, applications and services. (2007), pp. 233–245. https://doi.org/10.1145/1247660.1247688
19. M. Gruteser, X. Liu, Protecting privacy, in continuous location-tracking applications. IEEE Security & Privacy. 2(2), 28–34(2004). https://doi.org/10.1109/MSECP.2004.1281242
20. J. Meyerowitz, R. Roy Choudhury, Hiding stars with fireworks: location privacy through camouflage. in: Proceedings of the 15th annual international conference on Mobile computing and networking. (2009), pp. 345–356.
21. N. Shen, J. Yang, K. Yuan, C. Fu, C. Jia, An efficient and privacy-preserving location sharing mechanism. Computer Standards & Interfaces. 44, 102–109(2016). https://doi.org/10.1016/j.csi.2015.06.001
22. J. Chen, S. Su, X. Wang, Towards privacy-preserving location sharing over mobile online social networks. IEICE TRANSACTIONS on Information and Systems. 102(1), 133–146(2019). https://doi.org/10.1587/transinf.2018EDP7187
23. W. Wei, F. Xu, Q. Li, Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. in: 2012 Proceedings IEEE INFOCOM. (2012), pp. 2616–2620. https://doi.org/10.1109/INFCOM.2012.6195664
24. J. Li, J. Li, X. Chen, Z. Liu, C. Jia, Mobishare+: Security improved system for location sharing in mobile online social networks. J. Internet Serv. Inf. Secur. 4(1), 25–36(2014).
25. Z. Liu, J. Li, X. Chen, J. Li, C. Jia, New privacy-preserving location sharing system for mobile online social networks. in: 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. (2013), pp. 214–218.
26. Z. Liu, D. Luo, J. Li, X. Chen, C. Jia, N-mobishare: new privacy-preserving location-sharing system for mobile online social networks. International Journal of Computer Mathematics. 93(2), 384–400(2016). https://doi.org/10.1080/00207160.2014.917179
27. G. Sun, Y. Xie, D. Liao, H. Yu, V. Chang, User-defined privacy location-sharing system in mobile online social networks. Journal of Network and Computer Applications. 86, 34–45(2017). https://doi.org/10.1016/j.jnca.2016.11.024
28. J. Li, H. Yan, Z. Liu, X. Chen, X. Huang, D. S. Wong, Location-sharing systems with enhanced privacy in mobile online social networks. IEEE Systems Journal. 11(2), 439–448(2015). https://doi.org/10.1109/JSYST.2015.2415835
29. C. Xu, X. Xie, L. Zhu, K. Sharif, C. Zhang, X. Du, M. Guizani, PPLS: a privacy-preserving location-sharing scheme in mobile online social networks. Science China Information Sciences. 63(3), 1–11(2020). https://doi.org/10.1007/s11432-019-1508-6
30. X. Xiao, C. Chen, A. K. Sangaiah, G. Hu, R. Ye, Y. Jiang, Cenlocshare: a centralized privacy-preserving location-sharing system for mobile online social networks. Future Generation Computer Systems. 86, 863–872(2018). https://doi.org/10.1016/j.future.2017.01.035

Figures

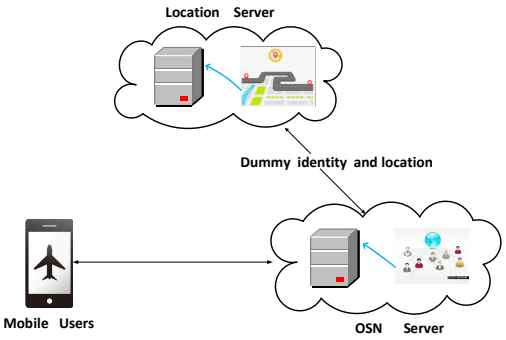

Figure 1: System architecture in mobile online social networks(mOSNs)

Mobile User (u_i)	*Online social network Server* (S_{OSN})	*Location Server* (S_{LS})
(pk_{ID_i}, sk_{ID_i})	*social network graph G* $(ID_i, df_{ID_i}, ds_{ID_i}, pk_{ID_i})$ (pk_{osn}, sk_{osn})	(pk_{LS}, sk_{LS})

$\sigma_{ID_i} = Sig_{sk_{ID_i}}(ID_i, ts)$

$c_{ID_i} = E_{pk_{osn}}(ID_i, ts, \sigma_{ID_i})$

$c = E_{pk_{LS}}(x, y)$

$\xrightarrow{(c_{ID_i}, c)}$

$(ID_i, ts, \sigma_{ID_i}) = D_{sk_{osn}}(c_{ID_i})$

If $(Ver_{pk_{ID_i}}(\sigma_{ID_i}) = (ID_i, ts))$

S_{OSN} *randomly generates a dummy identity* FID_i

and stores this updated record $(ID_i, FID_i, df_{ID_i}, ds_{ID_i}, pk_{ID_i})$

$\xrightarrow{(FID_i, c)}$

$(x, y) = D_{sk_{LS}}(c)$

store the record $(FID_i, (x, y))$

Figure 2: User registration in online social network server and location server

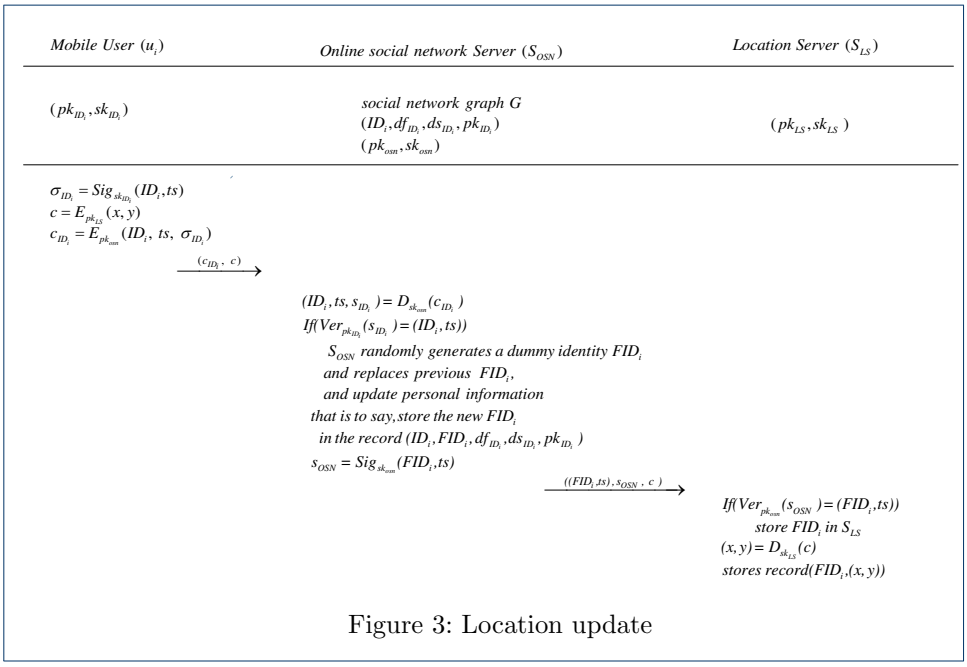

Figure 3: Location update

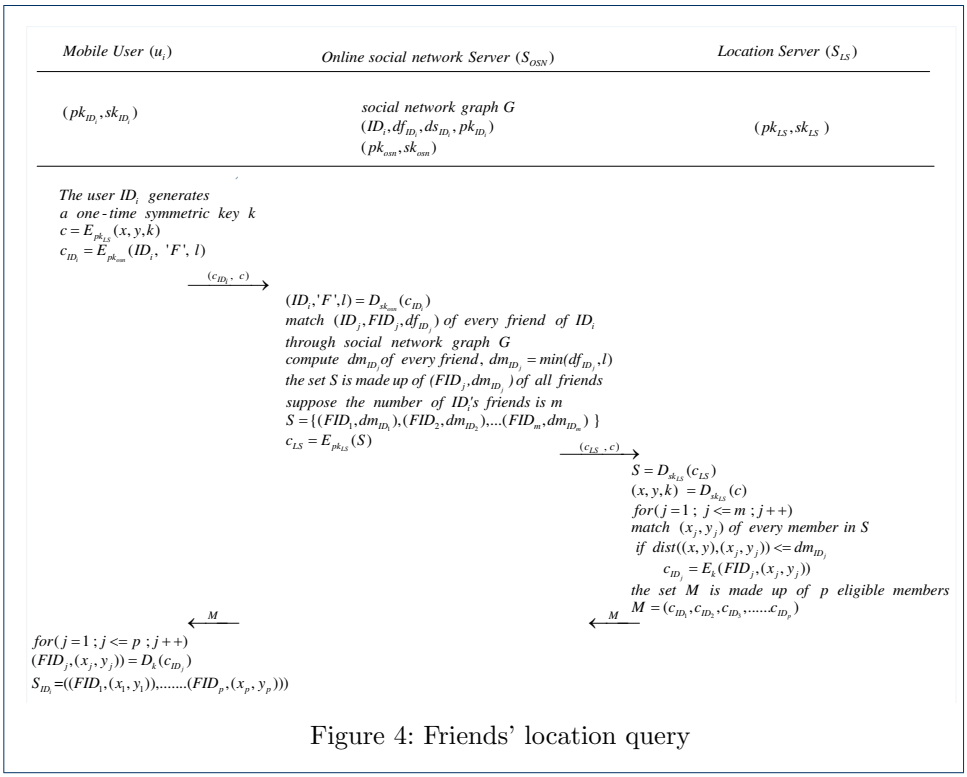

Figure 4: Friends' location query

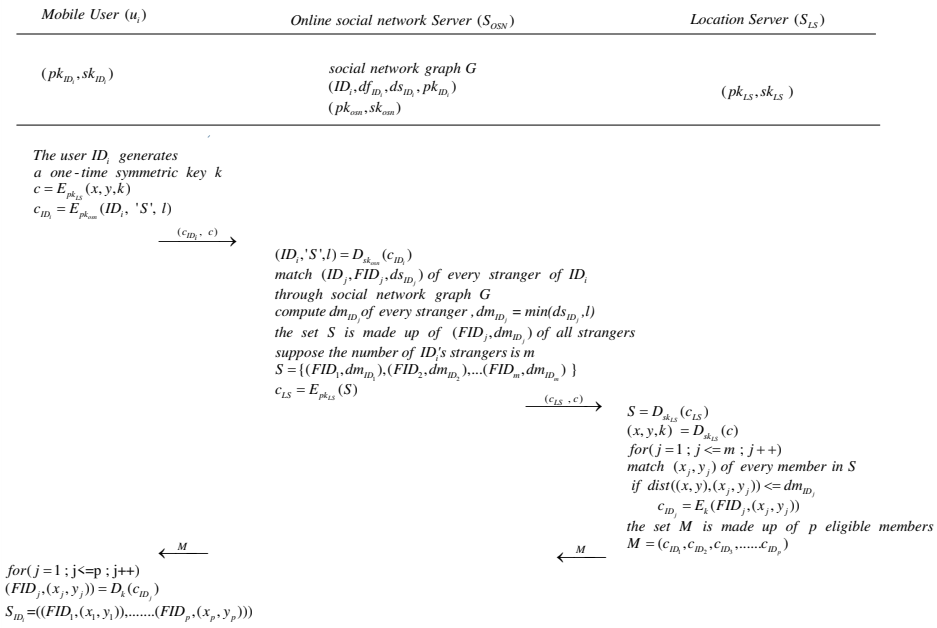

Figure 5: Strangers' location query

Figures

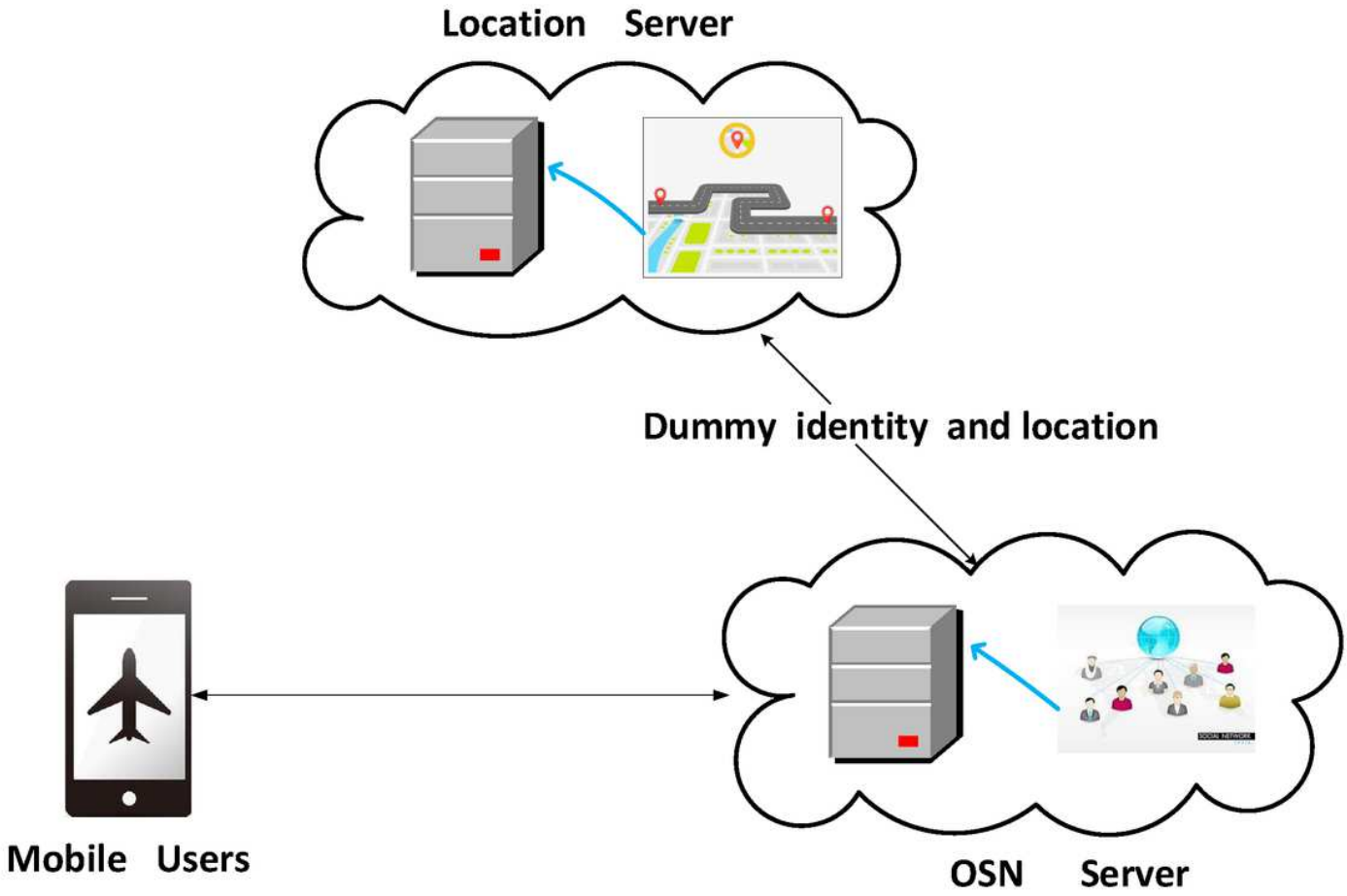

Figure 1

System architecture in mobile online social networks(mOSNs)

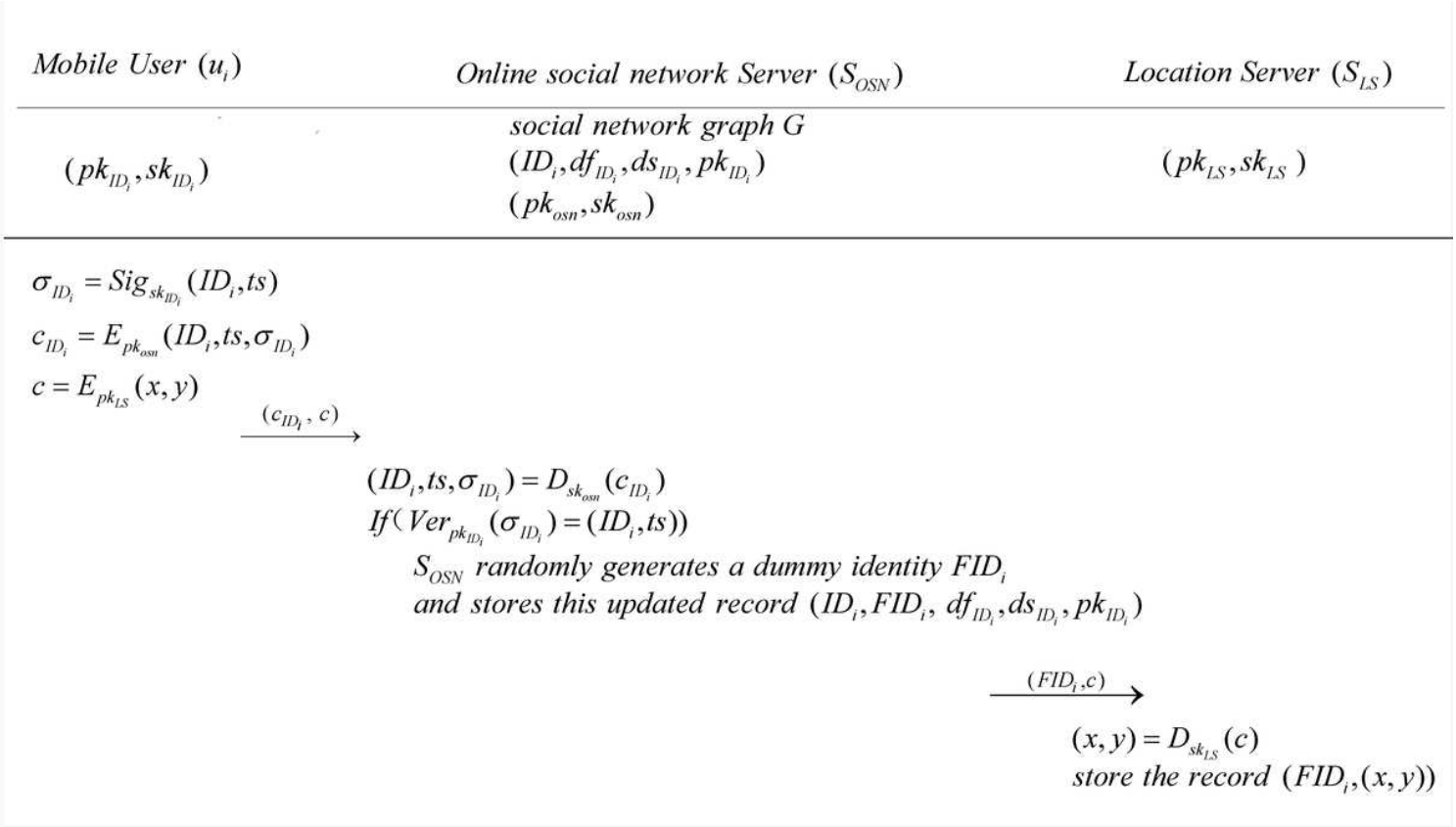

Figure 2

User registration in online social network server and location server

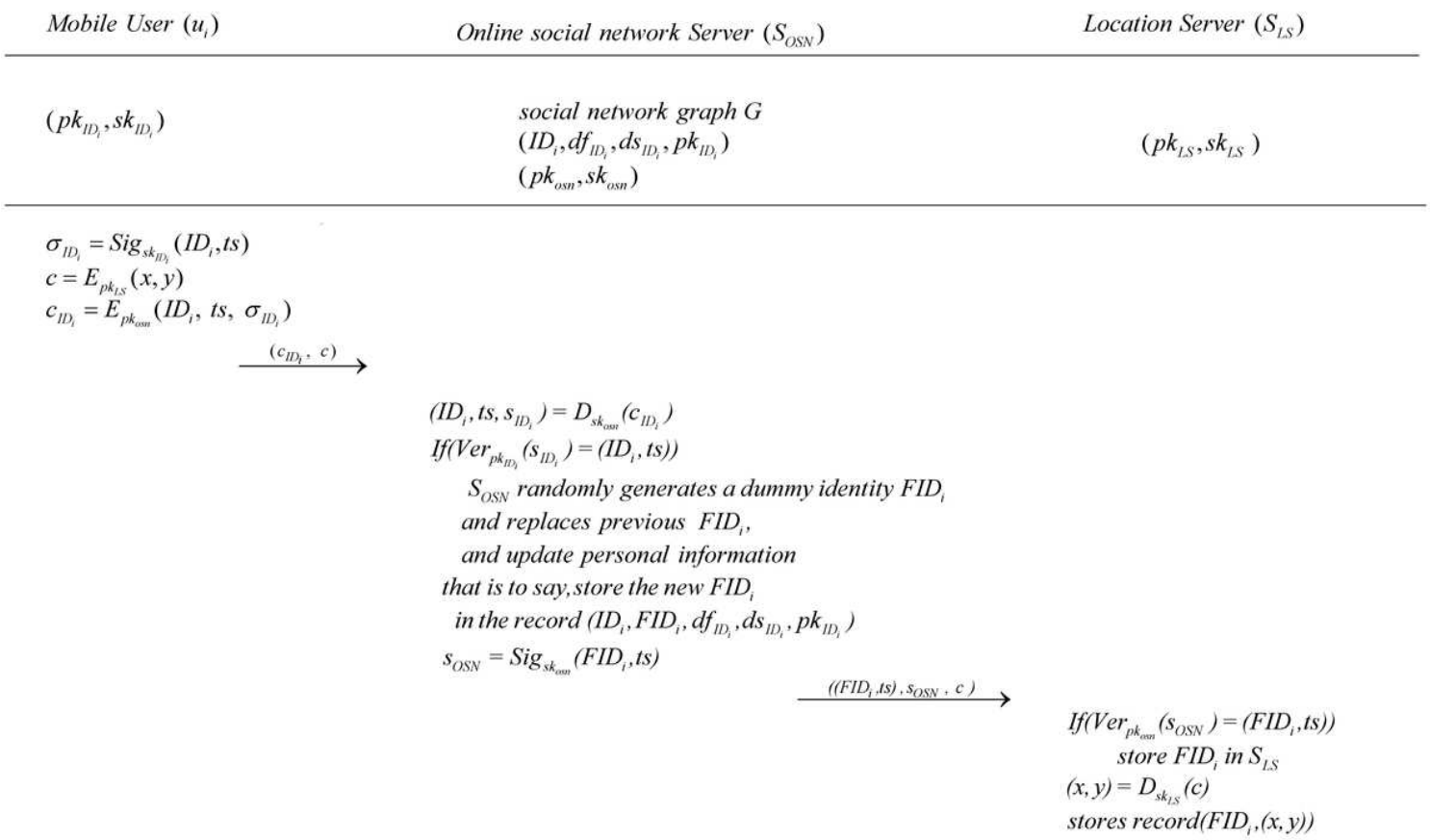

Figure 3

Location update

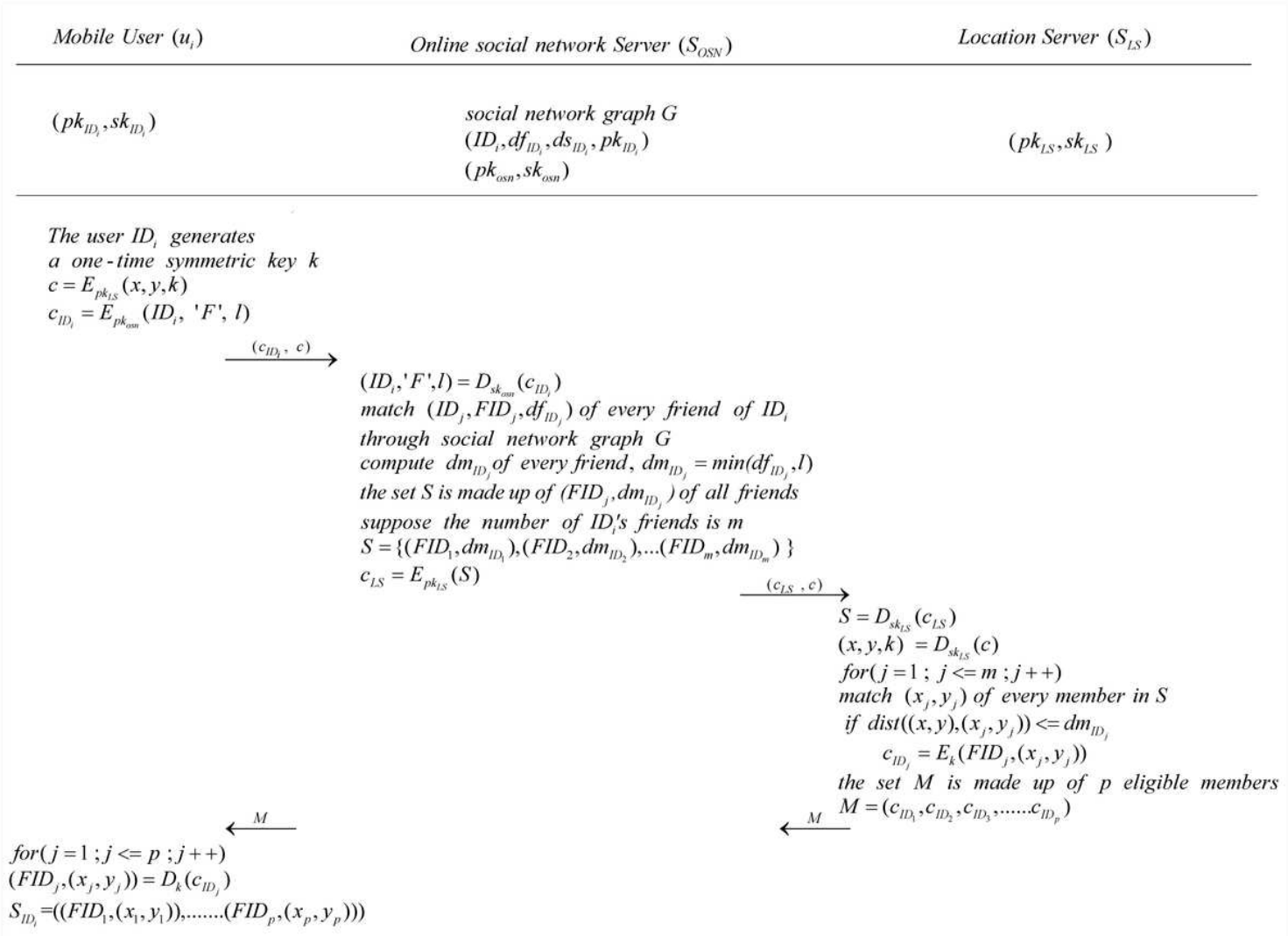

Figure 4

Friends' location query

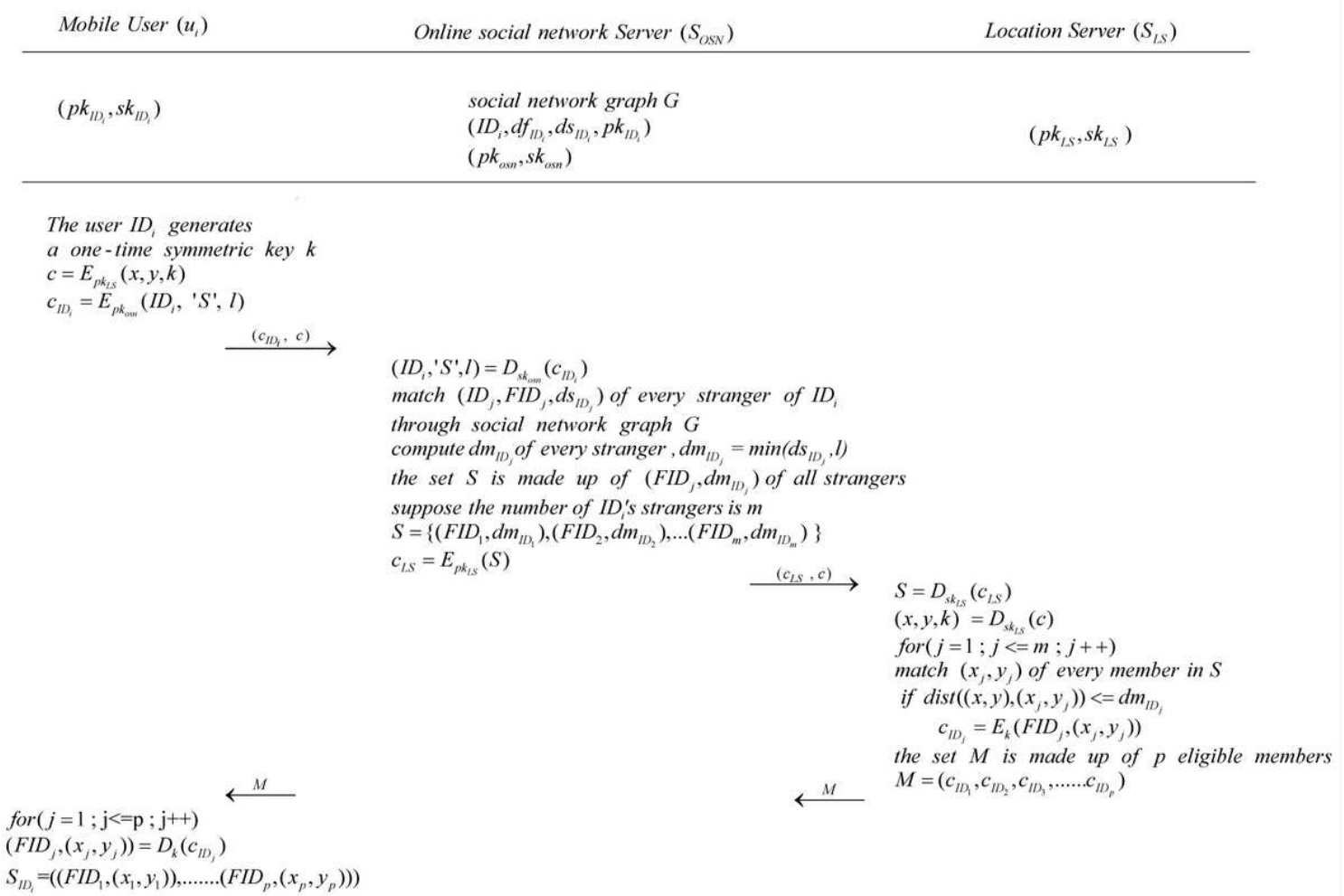

Figure 5

Strangers' location query