Journal of Computers Vol. 30 No. 3, 2019, pp. 59-71
doi:10.3966/199115992019063003005

IM-MobiShare: An Improved Privacy Preserving Scheme Based on Asymmetric Encryption and Bloom Filter for Users Location Sharing in Social Network

Lin Teng[1], Hang Li[1*], Shoulin Yin[1]

[1] Software College, Shenyang Normal University, No. 253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034-China
1532554069@qq.com; 910675024@qq.com; ysl352720214@163.com

Received 19 August 2017; Revised 4 December 2017; Accepted 1 February 2018

Abstract. Users location sharing in social network has become a hot issue nowadays. Traditional privacy preserving schemes are easily attacked by Hacker, which can result in leaking of sensitive information. And in the case of fewer users or shorter stay time, the information sharing efficiency is low and the privacy protection effect is not obvious. Some researchers proposed MobiShare scheme to solve this disadvantage, nevertheless, the cost of cellular tower in MobiShare system is too high lacking of practicability. MobiShare is a location-based service that assists users with searching and sharing files. To address the above problems, this paper proposes an improved privacy preserving scheme by improving MobiShare for the users location sharing in social network. Firstly, we optimize the traditional structure of MobiShare. Additionally, asymmetric encryption and Bloom filter are combined to enhance the security and efficiency of new scheme. Finally, performance and security analysis are proved to illustrate the availability of our new scheme. Experimental results show that our improved MobiShare scheme displays a better effectiveness for privacy preserving scheme.

Keywords: asymmetric encryption, bloom filter, location sharing, MobiShare scheme, privacy preserving

1 Introduction

Currently, mobile Internet technology experiences an advanced development, a new direction——mobile online social networks (MOSN) is developed [1-2]. Mobile users can enjoy various of services provided by MOSN as long as terminals are online. One of the most widely used services is location-based service. For example, the user can obtain the user's location coordinates automatically through the intelligent mobile terminal, and upload them into the related server [3]. Then detailed information about the hotels, cinemas and other places of interest around a certain range can be obtained.

As an important extension of location service in MOSN, location sharing has attracted more attention by users. By sharing their location information, users can real-timely obtain the position and status of other friends in the social network, which greatly improves the communication between users. While enjoying the convenience, the privacy protection of users cannot be ignored, especially for the leakage of users' sensitive real-time location and social network information. At present, most of the MOSN will collect users' real-time location information in the background server with different degrees and store them to analyze and process. This leads to potential risks, because once these servers cannot be trusted or they are attacked, it will result in leakage of massive users' privacy data. If a malicious attacker has mastered the information, they can obtain a large number of private information, such as the user's social relations, real-time location, habits and so on, the consequence will be unimaginable.

In order to protect the privacy of location sharing in MOSN, some solutions have been put forward, such as Mobishare scheme [4-6]. In this scheme, it allows users to customize access rules and query

* Corresponding Author

range, that can provide location sharing service between strangers and friends. In the architecture of Mobishare system, cellular tower is widely used for preprocessing users' location information. Additionally, the privacy information of users is protected by introducing the K-anonymous in cryptography. However, these measures have a certain risk, the cost of cellular tower is too high lacking of practicability. While the K-anonymous mechanism will occupy a large amount of storage space, sometimes the safety of K-anonymous is poor. Therefore, this paper proposes an improved privacy preserving scheme based on asymmetric encryption and bloom filter for users location Sharing in social network. So the Highlights in this paper is as:

- Drawbacks of traditional privacy scheme accounting for the weak robustness of the Mobishare scheme are revealed.
- An improved Mobishare scheme based on asymmetric encryption and bloom filter is proposed.
- The improved scheme achieves a good security effectiveness compared with state-of-the-art privacy preserving schemes.

2 Related Works

The widely use of users location coordinates in mobile online social networks will inevitably lead to security issue of location privacy. Currently, there are some related research results, such as anonymous technology [7], information hiding technology [8] and so on. There are two main location privacy protection schemes:

K-anonymous. By mixing a real user's location information into other anonymous users' location information, attacker cannot distinguish them. K-anonymous was put forward by Goyal in 2006 [9], and then Gruteser [10] and other researchers introduced it into location privacy protection. Yang et al. [11] extended this method and introduced the concept of virtual location. However, they do not consider the effect of quasi-identifier on different sensitive attribute. To a certain extent, that can lead to the leakage of sensitive data. Liu et al. [12] proposed a density-based clustering method for K-anonymity privacy protection. They also analyzed the effect of identifier on sensitive properties. Density clustering method was used to make sensitive properties cluster for data, which made the data more similarity in same class. Through this new clustering method, it could make differentiation for query function sensitive properties and improve data availability. Yin et al. [13] presented a new social network privacy protection based on a new Map-Reduce model with a k-means approach. Main task controlled k-means to start iterative execution.

Position encryption. Using some mature encryption algorithms to encrypt location coordinates. For example, Kim et al. [14] proposed a Hilbert curve-based cryptographic transformation scheme to preserve the privacy of the spatial data from various attacks on outsourced databases. Cui et al. [15] presented a novel Hierarchical Hilbert curve spatial cloaking algorithm to effectively achieve K-anonymity for mobile users in location-based services. Although, they make an improvement on position encryption, robustness and time complexity is poor. Lan et al. [16] put forward a new security cloud storage data encryption scheme based on identity proxy re-encryption. This scheme could flexibility share data with other users security without fully trusted cloud. For the detailed structure, they used a strong unforgeable signature scheme to make the transmuted ciphertext have publicly verification combined identity-based encryption. Yin et al. [17] showed a searchable asymmetric encryption scheme which could effectively search data on encrypted data. It was also a way to share the position information with protection.

Bilogrevic et al. [18] presented SPISM, a novel information-sharing system that decided (semi-) automatically, based on personal and contextual features, whether to share information with others and at what granularity, whenever it was requested. SPISM made use of (active) machine-learning techniques, including cost-sensitive multi-class classifiers based on support vector machines. SPISM provided both ease of use and privacy features. It adapted to each user's behavior and predicted the level of detail for each sharing decision. Zhang et al. [19] designed a Prophet framework, which provided an effective security scheme for users sharing their location information. First, they defined fingerprint identification based on Markov chain and state classification to describe the users' behavior patterns. Then, they proposed a novel location anonymization mechanism, which adopted a ε -indistinguishability strategy to protect users' sensitive location information published. But, this method can cost plenty of time. Aiming

to improve the above problems, we propose the new scheme.

Our contribution. In this paper, we design an improved BMobishare users location sharing privacy protection scheme. Compared with the traditional BMobishare scheme, the structure of new scheme is optimized, which weakens the function of cellular tower. New scheme conforms to the characteristic of social network service deeply. Through removing K-anonymous mechanism and introducing asymmetric encryption system and Bloom filter, it further improves the safety and efficiency of the new scheme.

The remainder of this paper is organized as follows. Section 2 presents the related works. In Section 3, BMobishare scheme is analyzed first, then the improved BMobishare scheme is assessed. Section 4 presents the security analysis of improved scheme. In Section 5, performance evaluation is illustrated for our scheme. Conclusion is provided in Section 6.

3 Improved Privacy Preserving Scheme: IM-BMobishare

3.1 BMobishare Scheme

The architecture of Mobishare scheme is shown as Fig. 1. It mainly consists of four parts: user, social network server, position server and cellular tower.

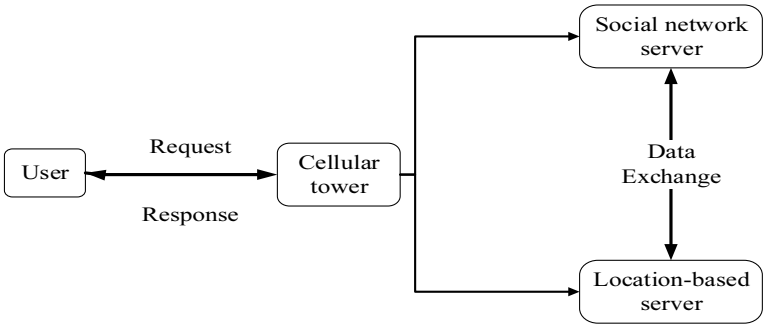

Fig. 1. Structure of Mobishare

Mobishare scheme combines the social network server and the location server. The server and cellular tower are connected by high speed and safe line. In Mobishare scheme, location query operations can be divided into friends location query and strangers location query. Users can share their location information with other users or the third party server. Additionally, social network server or location server cannot get all the information about the identity of the user, the user social relations and the corresponding real time position coordinates information.

3.2 Shortcomings of Mobishare Scheme

Although Mobishare scheme provides a location sharing privacy protection scheme between friends and strangers, there are still some demerits detailed described as follows.

The cellular tower is very powerful. In Mobishare scheme, cellular tower is a very important link. It not only needs to process the user's query information, but it is responsible for establishing connection security channel with other two servers. But in the actual situation, the coverage of each cellular tower is limitation. In order to achieve universal location sharing service, it needs to deploy a sufficient number of cellular towers, especially these cellular towers may belong to different operating companies. According to the Mobishare scheme, once the system needs to be upgraded, it requires amount of time and money, which is not practical.

K-anonymous technology is with hidden dangers. When updating the users location, submitting list of friends or querying the location information, cellular tower, social network server and location server in the Mobishare scheme need K-anonymous processing and fill with $k-1$ false information, which greatly affects the efficiency of the scheme. K-anonymous is also with less security. Shokri et al. [20] had designed an evaluation system to compare various privacy protection schemes. In this evaluation system, K-anonymous technology could only reduce the probability of successful attacking belonging to the lower protection level.

Recently, Li et al. [21] improved Mobishare scheme by using privacy interaction protocol of polynomial coefficients to construct the scheme. Although it could effectively improve the safety, it needed much more time.

3.3 Structure of Improved Mobishare System

In order to overcome the shortcomings of Mobishare scheme, this paper proposes an improved BMobishare scheme. The structure of new BMobishare scheme is shown in Fig. 2. It consists of users, social network server and location server.

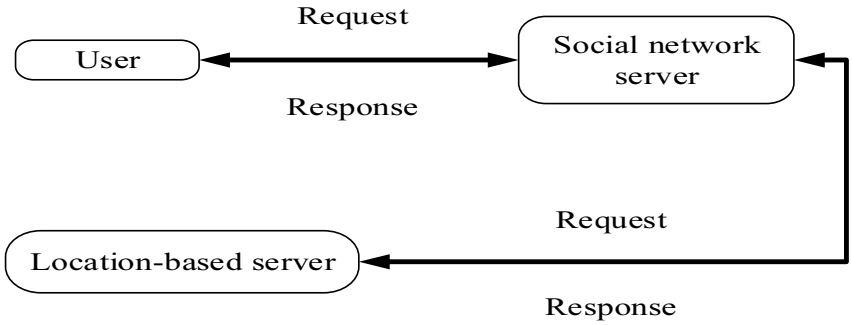

Fig. 2. Structure of new Mobishare system

The social network server is responsible for storing and processing all the information related to the users' identity including ID, users' friend list. The location server is responsible for storing and processing users location information which can be provided by a specific location service company or deployed in a public cloud.

Users who have registered MOSN services can use their mobile clients to acquire communication service through 3G / 4G wireless communication technology and cellular towers around the world. However, in the new BMobishare scheme, the cellular tower no longer provides any function of storing and processing users information, it only serves as a connection for forwarding information, so it can be ignored in Fig. 2. The operation of users location information will be performed by the users' mobile terminal.

The new BMobishare scheme adopts an irreversible hash function and two encryption methods: public key encryption and asymmetric key encryption. There are many irreversible hash functions, and our new scheme adopts Secure Hash Algorithm1 (SHA1). Public key encryption technology uses a pair of asymmetric keys for encrypting and decrypting operation, RSA algorithm is adopted in this paper. And asymmetric key encryption technology uses the different key for data encryption and decryption operation, but the paper uses AES method in the two operations.

In addition, the new scheme also utilizes a Bloom filter in the social network server and location server to hide sensitive information. Bloom filter is a binary vector data structure, the space and time efficiency is better. It is usually used for detecting whether an element belongs to a given set. If determining whether an element belongs to a set, the common method is to save all the elements, and then comparing them. However, if the number of elements in the set becomes larger, then the time and space required for detection will become larger too, that can result in a significant reduction of detection efficiency. In contrast, if Bloom filter is used to detect, the advantage is that elements insertion and query time are constant. Furthermore, the query operation does not need to save the elements, it has better security.

3.4 Threat Model

In the new BMobishare system, a high-speed and secure line connects social network server and location server. In order to prevent malicious access, the user cannot directly access to the location server. Social network servers and location servers are "honest but curious". On the one hand, they can faithfully complete their work, on the other hand, they want to get more information about user. In this article, we further separate the social network server and location server. In other words, they cannot be controlled by an attacker at the same time.

Additionally, malicious users may also be associated with the social network server or location server

collusion to illegally acquire users' information. Both of these situations are likely to occur. For example, a malicious user illegally invades a server to steal the data. A technical personnel of social network server registers location sharing service, they can use their authority to implement illegal malicious attacking.

3.5 Design of New Scheme

This paper processes the location sharing protection from two aspects: location sharing of friends and location sharing of strangers. The new BMobishare scheme consists of five phases: user registration, building secure connection, location update, friends location query, and strangers location query. The following subsections will detailed introduce the new BMobishare scheme, which involves symbols shown in Table 1.

Table 1. Symbols in this paper

Symbol	Description
hash	One irreversible Hash function
ID_M	Unique identity ID of user M
FID_M	A fake ID of user after hash processing
tdf_M	Threshold distance set by user M in friends location query
tds_M	Threshold distance set by user M in strangers location query
S_M	Asymmetric key of user M
cp_M	Current position coordinates of user M
Pub_{LS}	Public key of location server
$\Pr i_{LS}$	Private key of location server

We would like to stress that the class/style files and the template should not be manipulated and that the guidelines regarding font sizes and format should be adhered to. This is to ensure that the end product is as homogeneous as possible.

3.5.1 User Registration

Before location-sharing, each user needs to register on the social network server and then get unique identity code ID_M. For each registered user M, the social network server will use an irreversible hash function *hash* to transform the ID_M and generate a fake ID of M, namely $FID_M = hash(ID_M)$, and it will be stored in a list $list_{\inf}$. In addition, the user M must send his friends list $frend_{list}$ and access parameter setting (tdf_M, tds_M) to the social network server. Friends of M must be the registered users in the social network server. Access parameter setting refers to the threshold distance of location sharing service in different situations. tdf_M is the threshold distance that user M is willing to share the location with his or her friends. If the distance between a friend and user M is greater than tdf_M, he cannot obtain the current position coordinates of user M. tds_M is the threshold distance that user M is willing to share the location with a stranger. If the distance between a stranger and user M is greater than tds_M, then he cannot get the current position coordinates of user M. $frend_{list}$ will be stored in the social network server, FID_M and (tdf_M, tds_M) will be sent to the location server and stored in table $local_{\inf}$.

It is worth noting that the access parameter (tdf_M, tds_M) can be reset by user M according to the actual situation. For example, if user M sets (tdf_M =0, tds_M =0), which means that user M does not want anyone to get his position coordinates, called "stealth" state. The process of user registration is shown in Fig. 3.

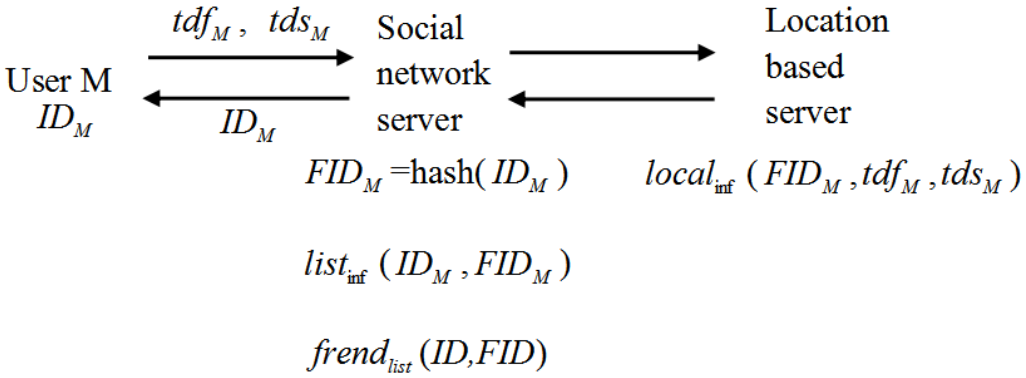

Fig. 3. Process of user registration

3.5.2 Building Secure Connection

After users registration, it is necessary to establish a secure connection between user M and location server. Once the location server receives the FID_M from M and (tdf_M , tds_M), it will automatically generate a pair of public key Pub_{LS} and private key $\Pr i_{LS}$ based on RSA. And it sends the public key Pub_{LS} to the user M. After user M receives the Pub_{LS} , it encrypts asymmetric key S_M , and then returns the encrypted information $Pub_{LS}(S_M)$ to the location server. After receiving the $Pub_{LS}(S_M)$, location server uses the private key $\Pr i_{LS}$ to decrypt it, and gets the asymmetric key S_M . Finally, the location server disposes the Pub_{LS} and $\Pr i_{LS}$ in this transition process. Thus, a secure connection based on asymmetric key S_M is established between user M and location server.

Note that the asymmetric key S_M is updated regularly, when user M resets his own information, the system can automatically update asymmetric key S_M to ensure the security of connection. The process of establishing a secure connection is shown in Fig. 4.

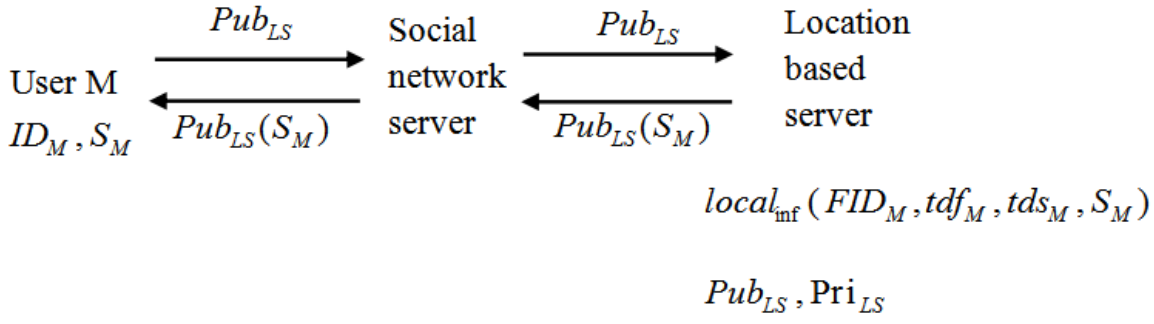

Fig. 4. Process of building secure connection

3.5.3 Location Update

User M will periodically obtain his own real-time position coordinates through GPS positioning technology. Once the location coordinates have been changed, user M will generate a location update message $(ID_M, S_M(cp_M))$ and sent it to the social network server. Where cp_M is the current position coordinate of user M encrypted by asymmetric key S_M .

The social network server finds the FID_M corresponding to ID_M and replaces it. $(ID_M, S_M(cp_M))$ is sent to the location server. After receiving the location update information, location server searches the corresponding asymmetric key S_M in table $local_{\inf}$ through FID_M , and decrypts it. Then it gets and stores cp_M .

In order to improve the efficiency of query, $local_{\inf}$ storing user coordinates in location server will be periodically rearranged. The adjacent user records of position coordinates are stored in the adjacent term of table. In this way, when it executes the process of location-sharing query in a certain area, it is easy to find the items that meet the conditions from the table only by scanning the continuous data, which greatly improves the query response time. The process of location update is shown in Fig. 5.

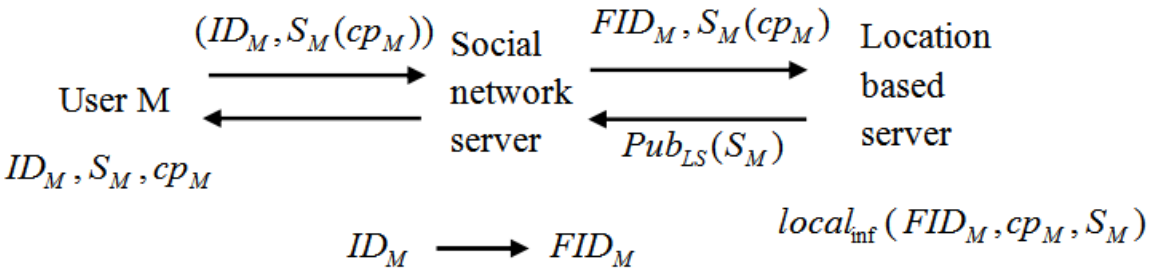

Fig. 5. Process of location update

3.5.4 Friends Location Query

In order to conduct a secure, efficient friends location query, the new scheme will build a privacy protection between the social network server and location server by establishing a Bloom filter. The process of friends position query mainly consists of four steps:

(1) User M sets the range of friends query and submits query request $(ID_M, S_M(cp_M, seq), r, 'f')$ to the social network server. Where cp_M is the current position coordinate of user M, seq is the sequence verification number, 'f' indicates that the query is a friend location query.

(2) After receiving the query, the social network server, on the one hand, replaces the ID_M by FID_M. On the other hand, it finds the friends list $frend_{list}$ of ID_A. Then FID_M and $frend_{list}$ will be inserted into Bloom filter (BF) in turn. $(FID_M, S_M(cp_M, seq), r, 'f', BF)$ will be sent to location server.

(3) The location server finds the corresponding record through FID_M and gets the key to obtain the location coordinate cp_M and sequence verification number seq. Then it finds out all the records in $local_{\inf}$. For each searched record, it needs to be filtered by comparing the friend threshold distance tdf_M. The location server will execute Bloom filter for FID that meet the conditions in the record item. The extracted record items constitute table $frend_{list}1$. Where $frend_{list}1 = (FID_1, FID_2, \cdots, FID_{m1})$, $m1$ is the number of found record items. Similarly, the coordinates corresponding to each item in table $frend_{list}1$ are encrypted by asymmetric key S_M to generate table $Location_{list}1$, where $Location_{list}1 = (S_M(cp_1), S_M(cp_2), \ldots, S_M(cp_{m1}))$. The location server returns the query result $(friend_{list}1, location_{list}1, seq)$ to social network server.

(4) After receiving the query results, social network server will compare all the records in table $frend_{list}1$ with their own friends list $frend_{list}$, and delete those who do not belong to the $frend_{list}$. Then it replaces the remaining FID by corresponding ID to generate table $frend_{list}2$. $frend_{list}2 = (ID_1, ID_2, \cdots, ID_{m2})$. Meanwhile, $Location_{list}1$ is also abbreviated to $Location_{list}2$, where $Location_{list}2 = (S_M(cp_1), S_M(cp_2), \ldots, S_M(cp_{m2}))$. Followed by that $(friend_{list}2, location_{list}2, seq)$ is returned to user M. Finally, the user M firstly checks the sequence verification number seq. If it is correct, it will use asymmetric key S_M to decrypt the result, and get the friends location information about surrounding r.

Detailed process of friends location query is shown in Fig. 6.

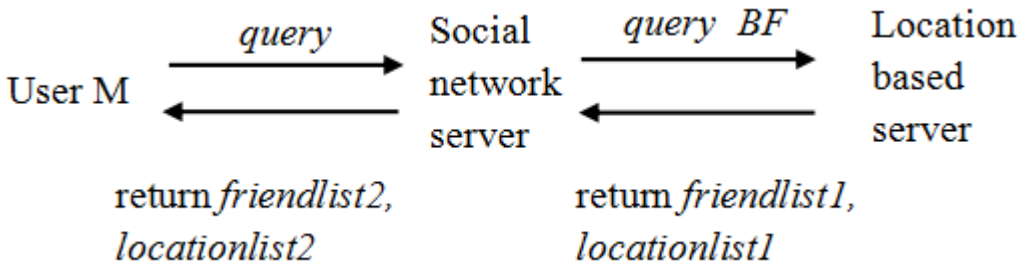

Fig. 6. Process of friends location query

3.5.5 Strangers Location Query

This process has similar phases with friends location query. However, it does not refer to finding friends list in social network server, which ignores the process of establishing a Bloom filter. The process of strangers position query mainly consists of four steps:

(1) User M sets the range r of friends query and submits query request $(ID_M, S_M(cp_M, seq), r, 's')$ to the social network server. Where cp_M is the current position coordinate of user M, seq is the sequence verification number, 's' indicates that the query is a stranger location query.

(2) After receiving the query, the social network server replaces the ID_M by FID_M. $(FID_M, S_M(cp_M, seq), r, 's')$ will be sent to location server.

(3) The location server finds the corresponding record through FID_M and gets the key to obtain the location coordinate cp_M and sequence verification number seq. Then it finds out all the records in $local_{\inf}$. For each searched record, it needs to be filtered by comparing the stranger threshold distance tds_M. The location server will extract FID that meet the conditions in the record item. The extracted record items constitute table FID_{list}. Where $FID_{list} = (FID_1, FID_2, \cdots, FID_n)$, n is the number of found record items. Similarly, the coordinates corresponding to FID_{list} in table $frend_{list}1$ are encrypted by asymmetric key S_M to generate table $Location_{list}$, where $Location_{list} = (S_M(cp_1), S_M(cp_2), \ldots, S_M(cp_n))$. The location server returns the query result $(FID_{list}, location_{list}, seq)$ to social network server.

(4) After receiving the query results, social network server will replace all the FID in FID_{list} by corresponding ID to generate table ID_{list}. $ID_{list} = (ID_1, ID_2, \cdots, ID_n)$. $(ID_{list}, location_{list}, seq)$ is returned to user M. Finally, the user M firstly checks the sequence verification number seq. If it is correct, it will use asymmetric key S_M to decrypt the result, and get the strangers location information about surrounding *r*.

4 Security Analysis

Improved BMobishare scheme set that social network server and location server are "honest but curious", they cannot be controlled at the same time by adversary, that is, they cannot collude with each other. This set is necessary, if they can collude with each other, then there is no privacy protection for users. Meanwhile, social network server or location server is likely to collude with a malicious registered user. We use analysis of two main threats and Bloom filter characteristic to prove the security of improved BMobishare scheme.

4.1 Location Privacy

A social network server or location server may collaborate with a malicious user and make an attempt to illegally obtain location information of a particular user. Because a malicious user can normally registered service, he could get some necessary information through legal methods, which makes him and the collaborated server can get plaintext and ciphertext to launch chosen plaintext attack or chosen

ciphertext attack. However, due to the limitation of user registration, malicious users can only obtain limited plaintexts and ciphertext pairs, so that the collaborated server cannot start dictionary attack. In that the improved BMobishare scheme makes encryption for location information of users. Furthermore, AES and RSA encryption system are security for chosen plaintext attack or chosen ciphertext attack, so improved BMobishare scheme is security too.

4.2 Social Relations Privacy

The location server may want to obtain all the social relationships of a particular user illegally. In the improved BMobishare scheme, the privacy protection of social relationships is realized by the security of Bloom filter in a friend location query. The social network server does not send the friends list directly to the location server, in contrary, it builds a related Bloom filter and sends it to the location server. Bloom filter can execute a convenient query operation. Whether an element belongs to a set, but it needs not to be saved, Bloom filter is with very good security. If adversary wants to attack the Bloom filter, he can only do exhaustive test, which is a large computation. It is infeasible. In addition, each query includes sequence verification related time, it can effectively prevent the replay attack and tamper attack. Therefore, improved BMobishare scheme is security.

4.3 False Alarm rate of Bloom Filter

It is worth noting that the Bloom filter has a certain false alarm rate. There may be some elements not in the detection set, but the testing results are still "yes". Although there is a certain false alarm rate, the Bloom filter will not miss any of the elements in the detection set. In other words, Bloom filter only can be with misstatement, but not underreporting.

Generally, the more elements are inserted, the false alarm rate will increase. Set n is the number of elements inserted into a Bloom filter. m is the length of the bit array to be detected. q is the number of independently hash functions used to map, the false alarm rate p can be described as,

$$p = (1 - (1 - \frac{1}{m})^{n,q})^q . \quad \textbf{(1)}$$

According to analysis of probability, if p reaches the minimum value, the optimal value of q is

$$q = (m/n)\ln 2 \ . \quad \textbf{(2)}$$

By introducing the optimal value of q , the relation between the length m of Bloom filter and the false alarm rate p is expressed as follows:

$$m = \left\lceil n((-loq_2^n)/\ln 2) \right\rceil . \quad \textbf{(3)}$$

Because the number of inserted elements n is the number of users' friends. For most ordinary users, n will be below 1000. Thus, the false positive rate p can be controlled completely. However, if the p value is very small, m will be too large. That is, the length of the Bloom filter is too large and more space resources will be occupied. After calculation, if $p = 10^{-2}$, m value is less than 105bit, this size is acceptable. And in the improved BMobishare scheme, the social network server receives the returned query results, it needs to make a filter operation in its own database, it is easy to filter out a very small number of false alarm elements.

5 Performance Analysis

5.1 Storage Consumption

Firstly, the storage consumption of each part of the system is compared. Since the system architecture of Mobishare and improved BMobishare scheme are same, they have the same storage consumption. So following analyzes the improved Mobishare scheme.

Assuming that the social network has a total of 2000 registered users, each user has 100 friends. There are 50 Cellular towers in one region. In order to implement K-anonymity, we select *k=10* [22] (If *k* is bigger, there is little effect on improving data quality, though they are the best k-anonymity algorithms. If *k* is smaller, the k-anonymous table may not satisfy users' privacy protection requirements, and the k-anonymous privacy protection model will lose its meaning). Each user's ID_M and FID_M are 18bit. Each coordinate cp_M and $S_M(cp_M)$, tdf_M and tds_M are 8bit. Asymmetric key of each ASE is 128bit.

For Cellular tower:

(a) Mobishare scheme requires to store $(ID_M, FID_M, tdf_M, tds_M)$ and 2 ASE keys of users, so each Cellular tower needs storage consumption: $(8\times2+18\times2)\times2000/50+2\times128=2.3\times10^3$bit.

(b) Improved BMobishare scheme completely weakens the cellular tower with a storage cost 0 bit.

For social network server:

(a) Mobishare scheme needs to store all users' $(ID_M, FID_M, friend_{list})$. As a result of using k-anonymous technology, so the required storage consumption is $(18\times3+18\times100\times10)\times2000=3.61\times10^7$bit.

(b) Improved BMobishare scheme cancels K-anonymous technology, so the required storage consumption is $(18\times3+18\times100)\times2000=3.7\times10^6$bit.

For location server:

(a) Mobishare scheme needs to store all users' $(FID_M, (cp_M), S_M(cp_M), tdf_M, tds_M)$ and 2 ASE keys. Due to K-anonymous technology, the required storage consumption is $(18+4\times8+128\times2)\times2000\times10=6.12\times10^6$bit.

(b) Improved BMobishare scheme eliminates k-anonymous method and reduces one ASE key, the required storage consumption is $(18+4\times8+128)\times2000=3.56\times10^5$ bits.

The above analysis is summarized as Table 2. Meanwhile, we compare our method with state-of-the-art schemes (including ELPP [23], IMPEE [24] PEPQ [25] and CFDC [26]) to demonstrate the effectiveness of our new method under the same environment with matlab2017, CPU2.2GHz, RAM8G. ELPP addressed the problem in location-based services that the disclosure of a user's real location while interacting with the location service provider. But it has a low effect in different environment. Although, the robustness of IMPEE is enhanced, the time consumption is high. PEPQ and CFDC combined other schemes, which cannot improve the security of location information. From Table 2, it notes that the improved BMobishare scheme has a significant reduction in the storage cost compared with the previous scheme. And new BMobishare scheme completely weakens the cellular tower, so the deployment and maintenance costs of system are greatly reduced, which enhances the practicality of new scheme.

Table 2. Storage cost

Scheme	Cellular tower	Social network server	Location server
Mobishare	2.3×10^3	3.61×10^7	6.12×10^6
ELPP	6.8×10^2	2.88×10^7	2.65×10^6
IMPEE	540	2.14×10^7	1.34×10^6
PEPQ	278	8.9×10^6	4.87×10^5
CFDC	266	5.5×10^6	4.08×10^6
Improved BMobishare	0	3.7×10^6	3.56×10^5

5.2 Time Consumption

In this subsection, we compare the time cost of improved BMobishare and Mobishare. Since the public key encryption in the new scheme only acts a function for exchanging the asymmetric key of the user and location server, only runs one time. It takes about 0.5s in the mobile terminal and does not take up the query time. While each query uses ASE to make asymmetric encryption, its security is much better than K-anonymous. And asymmetric encryption takes less time. Therefore, improved BMobishare scheme is theoretically more efficient than the previous scheme. In order to achieve better comparison effect, this paper adopts simulation experiments to verify. Unlike the previous scheme, the improved BMobishare scheme is fully operated at the application level, so it is easily inserted with the interface form. In this paper, the simulation experiments are carried out with Java. The mobile terminal is Android4.2 system HUAWEI Mate 9 Pro smart phone. For convenience and comparability of the experiment, user has the

same number of friends with (100,200,300) in each query respectively. Table 3 is the result of time consumption.

Table 3. Time cost

Scheme	Input size	Time/s
Mobishare	100	1.25
	200	1.75
	300	2.01
ELPP	100	1.21
	200	1.64
	300	1.89
IMPEE	100	1.15
	200	1.54
	300	1.63
PEPQ	100	1.02
	200	1.44
	300	1.52
CFDC	100	0.98
	200	1.37
	300	1.50
Improved BMobishare	100	0.98
	200	1.26
	300	1.49

In improved BMobishare scheme, it uses an irreversible hash function and two kinds of encryption modes: public key encryption and asymmetric key encryption. Where, the hash function adopts SHA1 and public key encryption uses RSA respectively. Asymmetric key encryption adopts ASE with 128-bit in this paper.

Table 3 shows that improved BMobishare scheme takes less time and is more efficient than other existing related research work.

6 Conclusions.

In this paper, we propose an improved BMobishare scheme under the mobile online social network environment. This new scheme not only makes users get location sharing services, but provides a good protection for the users' privacy information. Compared with original Mobishare scheme, improved BMobishare scheme has two main contributions: (1) The original Mobishare system uses the cellular tower to preprocess users' location information, but this cost of deployment and follow-up upgrade is too high. This new scheme modifies the system architecture and cancels the functions of cellular tower; (2) the Mobishare scheme uses K-anonymous technology to protect the privacy of users, nevertheless, it has low efficiency and security. New scheme adopts privacy protection scheme based on the combination of location encryption and Bloom filter, which is more practical and safer. However, the limitation of the work is that Bloom filter may not be the best, so the space complexity is high. Hence, location information sharing will be improved by more advanced machine learning methods in the future.

Acknowledgments

The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] 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)(2015) 439-448.

[2] X. Xiao, C. Chen, A.K. Sangaiah, CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks, Future Generation Computer Systems 93(2)(2017) 214-218.

[3] P. Shi, M. Fang, H. Lin, A method for information source locating with incomplete observation of online social network, in: Proc. International Conference on Identification, Information, and Knowledge in the Internet of Things, 2016.

[4] A.N. Khan, M.L.M. Kiah, M. Ali, BSS: block-based sharing scheme for secure data storage services in mobile cloud environment, Journal of Supercomputing., 70(2)(2014) 946-976.

[5] H.-C. Chao, T.-Y. Fan, Random-grid based progressive visual secret sharing scheme with adaptive priority, Digital Signal Processing 68(9)(2017) 69–80.

[6] W. Wei, F. Xu, Q. Li, MobiShare: flexible privacy-preserving location sharing in mobile online social networks, in: Proc. IEEE INFOCOM, 2012.

[7] X. Tian, Y. Wang, Y. Zhu, Y. Sun, Q. Liu, De-anonymous and anonymous technologies for network traffic release, in: Proc. International Conference on Applications and Techniques in Information Security, 2017.

[8] Y. Lei, Digital image information hiding technology based on lifting wavelet transform and image fusion, in: Proc. International Conference on Computer Engineering, Information Science & Application Technology, 2016.

[9] B. Bouchon-Meunier, Fuzziness and knowledge-based systems, International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems 21(6)(2003) 797-797.

[10] M. Gruteser, D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking, in: Proc. International Conference on Mobile Systems, Applications, and Services, DBLP, 2003.

[11] Y. Yang, Perceived k-value location privacy protection method based on LBS in augmented reality, International Journal of Security & Its Applications 9(4)(2015) 25-32.

[12] J. Liu, S.L. Yin, H. Li, L. Teng, A density-based clustering method for k-anonymity privacy protection, Journal of Information Hiding and Multimedia Signal Processing 8(1)(2017) 12-18.

[13] S.L. Yin, J. Liu, A k-means approach for map-reduce model and social network privacy protection, Journal of Information Hiding and Multimedia Signal Processing 7(6)(2016) 1215-1221.

[14] H.I. Kim, S. Hong, J.W. Chang, Hilbert curve-based cryptographic transformation scheme for spatial query processing on outsourced private data, Data & Knowledge Engineering 104(6)(2016) 32-44.

[15] N. Cui, X. Yang, B. Wang, A novel spatial cloaking scheme using hierarchical Hilbert curve for location-based services, in: Proc. International Conference on Web-Age Information Management, 2016.

[16] C.H. Lan, H. Li, S.L. Yin, A new security cloud storage data encryption scheme based on identity proxy re-encryption, International Journal of Network Security 19(5)(2017) 804-810.

[17] S.L. Yin, L. Teng, L. Liu, Distributed searchable asymmetric encryption, Indonesian Journal of Electrical Engineering and Computer Science 4(3)(2016) 684-694.

[18] I. Bilogrevic, K. Huguenin, B. Agir, A machine-learning based approach to privacy-aware information-sharing in mobile social networks, Pervasive & Mobile Computing 25(39)(2016) 125-142.

[19] G. Zhang, J. Qu, Z. Fang, Prophet: a context-aware location privacy-preserving scheme in location sharing service, Discrete Dynamics in Nature and Society, 2017(2017) Article ID 6814832.

[20] R. Shokri, G. Theodorakopoulos, J.Y. Boudec, Quantifying location privacy, IEEE Symposium on Security & Privacy 42(12)(2011) 247-262.

[21] J. Li, X. Chen, {MobiShare}+: security improved system for location sharing in mobile online social networks, J. Internet

Serv. Inf. Secur. 4(1)(2014) 25-36.

[22] B. Gedik, L. Liu, Protecting location privacy with personalized k-anonymity: architecture and algorithms, IEEE Transactions on Mobile Computing 7(1)(2008) 1-18.

[23] T. Peng, Q. Liu, G. Wang, Enhanced location privacy preserving scheme in location-based services, IEEE Systems Journal 11(1)(2017) 219-230.

[24] Z. He, Y. Zhang, F. Gao, An improved accurate monotonicity-preserving scheme for the Euler equations, Computers & Fluids 140(2016) 1-10.

[25] H. Zhu, R. Lu, C. Huang, An efficient privacy-preserving location-based services query scheme in outsourced cloud, IEEE Transactions on Vehicular Technology 65(9)(2016) 7729-7739.

[26] M. Grissa, A.A. Yavuz, B. Hamdaoui, Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks, in: Proc. IEEE Computer Networks and Information Security, 2016.