RESEARCH ARTICLE OPEN ACCESS

Location Sharing System Using GPS Technology for Minimizing SMS Delivery

[1]C.Manikandan, [2]R.Selvamatha
[1](ME Scholar, Department of Computer Science, S.Veerasamy Chettiar College of Engineering and Technology, Puliyangudi-627855)
[2](Assistant Professor, Department of Computer Science, S.Veerasamy Chettiar College of Engineering and Technology, Puliyangudi-627855)

ABSTRACT
Enhanced Privacy in Mobile Online Social Networks to providing the location information to the User /server in the online location server. MOSNs, more and more users' location information will be collected by the service providers in mOSN. The users' privacy, including location privacy and social network privacy can be improved using the User Registration & encryption of the data stored into the server. It should aiming at achieving enhanced privacy against the insider attack launched by the service providers in mOSNs, we introduce a new architecture with multiple location servers for the first time and propose a secure solution supporting location sharing among friends and strangers in location-based applications. In our construction, the user's friend set in each friend's query submitted to the location servers is divided into multiple subsets by the social network server randomly. Location-based services (LBSs) are one of the most important components in mOSNs, which provides information and entertainment service based on the geographical position of the mobile device. The entity of users, with mobile devices, is able to communicate with other users and share their locations. Online social network Server manages users' identity-related information such as users' profiles and friend lists. Location server stores users' location information and provides LBSs according to the requests sent from users. Here we are going to improve the user location privacy, social network privacy.

Index Terms: Anonymity, checkability, insider threats, location privacy, location sharing, mobile social networks

I. INTRODUCTION
WITH the advent of mobile computing, traditional social networks have gradually become fresh paradigms called mobile online social networks (mOSNs). Much like the Location-based services (LBSs) are one of the most important components in mOSNs, which provides information and entertainment service based on the geographical position of the mobile device [2]. LBS has experienced explosive growth in recent years, particularly leveraging the fast development of mobile technology and the cloud computing. In LBS, the location of a device, representing one of the most important contextual information about the device and its owner, is exploited to develop innovative and value-added services to the users' personal context. Many individual, commercial, and enterprise-oriented LBSs are already available and have gained popularity. Various LBS applications have been proposed, such as location-based mobile advertising to mobile phone users. In E-health systems, LBS can also be applied to allow access to patient records outside the hospitals by doctors with locationbased access technology. There are also many examples of LBS including mobile check-in games like Foursquare [3], social networks like Loopt [4], and location-enabled applications like Google Maps. Analysts project the revenues for LBS to grow from 2.8 billion in 2010 to hit 10.3 billion by 2015.

1) We observe that the identity of the same querying user is linkable by the location service provider in the friends' location query of previous works [6]. Although multiple fake identities have been inserted for each user in these systems, friends' queries from the same user will be linked because of the same friend set. As a result, this security vulnerability will potentially help the location service provider identify which record is true in the location database and make location dummies useless. In addition, with the real fake identity, the location service provider can obtain the friend relations and locations even if some of them are dummies. More seriously, if we consider multiple queries without location updates, the location service provider is able to finally obtain the topological structure of the social network and launch multiple attacks.

2) Aiming at fixing this security issue, we propose a new system by introducing a new architecture with multiple location servers. More specifically, all location information will be stored in each location server. As a result, these queries cannot be linked to the same user, and improved privacy has been achieved in this new system.

When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

II. PROBLEM STATEMENT

Mobile security or mobile phone security has become increasingly important in mobile computing. It is of

Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

A. System Model

There are three entities in our mOSNs, which are described As follows.

1) *Users*. The entity of users, with mobile devices, is able to communicate with other users and share their locations with nearby friends and strangers.

2) *Online social network server*. This entity, denoted by $\mathcal{SOSN}$, manages users' identity-related information such as users' profiles and friend lists.

The $\mathcal{SOSN}$ provides online social network service to users based on the given identity-based information.

3) *Location Server*. This entity, denoted by $\mathcal{LS}$, stores users' location information and provides LBSs according to the requests sent from users.

B. Threat Model

Different trust assumptions will be defined over the entities involved in the system: 1) the users are assumed to be dishonest
and would try to access the location information outside the scope of their access privileges. 2) The social network server is assumed to be "honest-but-curious," i.e., the social network server will follow our proposed protocol but try to find out as much sensitive information as possible. For example, it may want to extract the users' location information from the interactive communications. 3) The location server is also supposed to be "honest-but-curious." It will also honestly follow our protocols and try to get some users' sensitive information such as the friend list.

Note that, in our security model, the adversary is not allowed
to control both the social network server and the location servers. In other words, the social network server and the location servers are not allowed to collude and get the information that they have not owned individually. This security assumption is also specified in [6]. This assumption is reasonable because it is unlikely that two service providers operated by independent organizations can be controlled by the same adversary.

particular concern as it relates to the security of personal information now stored on the smart phone.

More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks.

C. Security Goal

Based on the threat model defined previously, the following goals are defined for the location-sharing system in online mobile social networks.

1) For users, the system needs to protect their location privacy against the social network server and other unauthorized users (including both friends and strangers).

2) The location servers will provide the LBS to the users and should be prevented from getting the users' social network information.

3) The users' location information will be protected such that their friends or other strangers cannot access if their policy does not match the predefined access policy.

D. Symmetric Key Encryption

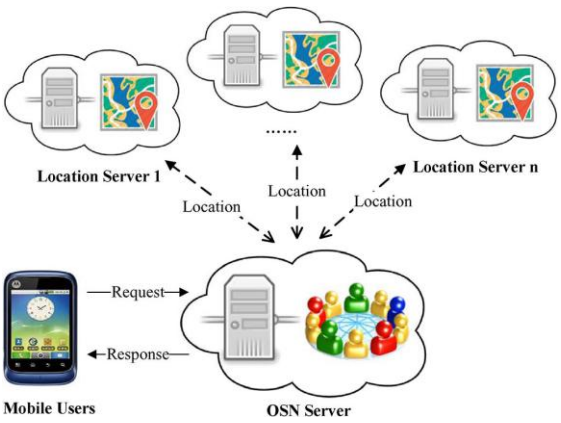
Symmetric encryption uses a common secret key κ to encrypt and decrypt data. A symmetric encryption scheme consists of three primitive functions.

1) $KeyGenSE(1\lambda) \rightarrow \kappa$ is the key generation algorithm that generates κ using security parameter 1λ.

2) $EncSE(\kappa,M) \rightarrow C$ is the symmetric encryption algorithm that takes the secret κ and message M and then outputs the ciphertext C.

3) $DecSE(\kappa,C) \rightarrow M$ is the symmetric decryption algorithm
that takes the secret κ and ciphertext C and then outputs the original message M.

III. BUILDING BLOCKS



A digital signature scheme is also required in our mechanism,
which is defined by the following three algorithms *KeyGen*, *Sign*, and *V erify*.

1) *KeyGen* is the key generation algorithm which takes input security parameter 1λ. It outputs (*pk, sk*) as a public/secret key pair.

2) *Sign* is the signing algorithm which takes input message *m* and secret key *sk* and outputs a signature σ.

3) *V erify* is the verification algorithm, which is given public key *pk*, message *m*, and signature σ as inputs and outputs accept if σ is a valid signature. Otherwise, output reject to denote that it is an invalid signature.

When working mobile, one is dependent on public networks, requiring careful use of VPN. Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.

When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life.

IV. SYSTEM ANALYSIS

1. Existing System

There are several ways to achieve the location privacy such as hiding the relations between user identity and location , location anonymity

Mobile devices or the trusted third server first processes location information through practical methods, such as encryption, to hide users' identity and then sends the results to the server provider to perform query.

These techniques of achieving location anonymity can be categorized into three types:

- *K*-anonymity
- Dummy locations.
- Location encryption

1.1 Disadvantages

Inaccuracy, imprecision, and vagueness. In location sharing in the online social networks

Cannot be guaranteed in this work without the trust assumption on the service providers.

2. Proposed System

To enhance the privacy in online social network system Users are required to register their personal information for the LBS at *S*OSN. Specifically, they need to provide the information of their profiles and individual preferences,

Users need to update their location information at the location servers if their locations change. The new location information will be stored and updated at the location servers for location services.

The Request will be classified into two types

- Friends Query
- Stranger's Query

2.1 Advantages

The location servers will provide the LBS to the users and should be prevented from getting the users' social network information.

The users' location information will be protected such that their friends or other strangers cannot access if their policy does not match the predefined access policy

Security & Accuracy will be enhanced using the OSN & cryptographic Symmetric Key encryption algorithm.

A broadcast encryption (BE) scheme is demanded in this paper. There are four algorithms defined in a BE scheme, i.e., *KeyGenBE*, *EncBE*, *DecBE*, and *RevBE*. Note that, in the BE scheme, it also provides a revocation function to protect the security against a coalition of all revoked users [11]. The description of the algorithms is as follows.

1) *KeyGenBE* is the key generation algorithm that is used to generate a long-lived key for the user.

2) *EncBE* is the encryption algorithm that is used to encrypt files to a privileged user group *G*.

3) *DecBE* is the decryption algorithm that is used to decrypt the ciphertext by authorized users. Assume that amessage is encrypted to a user group *G*. Then, it means that only users in group *G* can decrypt and get the message from the ciphertext.

4) *RevBE* is the revocation algorithm that is used to revoke the users from the broadcast user group *G*. Group *G* can be dynamically changing, as users can be added to or removed from *G*. If a user is removed from *G*, his privilege of decryption is also canceled. Thus, *DecBE* is the decryption algorithm that is only used to decrypt the ciphertext if with a nonrevoked secret key at the time the message was encrypted.

TABLE I
SUMMARY OF NOTATIONS

Symbol	Description
ID	User's social network identifier
$\mathcal{LS}$	Location server
$\mathcal{S}_{OSN}$	Social network server
$(x_{\mathrm{ID}}, y_{\mathrm{ID}})$	User ID's real location
FID	Fake identifier including real and dummy ones
df_{ID}	User ID's friend-case threshold distance
ds_{ID}	User ID's stranger-case threshold distance
qf	Distance threshold in friends' locations query
qs	Distance threshold in strangers' locations query
$k_{\mathcal{U}}$	A symmetric key shared by users
$\mathcal{G}$	A social network graph stored at $\mathcal{P}_{\mathrm{OSN}}$
$(pk_{\mathcal{U}}, sk_{\mathcal{U}})$	User's public key and secret key pair
$(pk_{\mathcal{LS}}, sk_{\mathcal{LS}})$	Location server's public and secret key pair

1) System Initialization: A symmetric key encryption scheme SE and a BE scheme BE are defined in the system. Each user has an identifier ID. The user generates and shares a symmetric key k with his friends. This symmetric key k will be encrypted and sent to all of his friends using the BE scheme. The user also prepares and registers a public key pair (PK,SK) for following registration/authentication. Assume that there are N location servers in our system.

2) Registration: There are two kinds of registration, which are specified as follows. *Social network service registration:* Before using the LBS in mOSN, each user needs to register for the service at the social network server. Suppose that $U = \{ID1, ID2, \ldots, IDn\}$ is the identity set of all of the users involved in the system, and a social network graph $G = (V,E)$ on U has been stored at $SOSN$, where $V \subseteq U$ is a set of identity vertices and $E \subseteq V \times V$ is a set of edges in G. Each user will define his access control policy by providing two threshold distances dfID and dsID. The value of dfID denotes which distance the user with identity ID is willing to share location with his/her friends, and dsID denotes the threshold distance within which he/she agrees to share location with strangers. After the registration,
the social network information and his/her friend relations at G are updated.

LBS registration: We assume that a location database in
the form of *{*(FID, (*x, y*), *df*ID, *ds*ID)*}* is maintained by *LS*, where FID is the user's pseudoidentity and (*x, y*) is his/her current location. Let (FID*i*, (*xi, yi*), *dfi*, *dsi*) be any valid record in the location database, dist(·, ·) be a distance function, and min(·, ·) return the minimum value in its inputs.
3) Location Updates: To update his/her location, the user with identity ID sends the information of (ID, *C*(*x, y*), *C*_(*x, y*)) and (*ts*, Sig*SK*ID(ID, *ts*)) to *S*OSN, where (*x, y*) is his current location, *C*(*x, y*) is the encryption on the location with the secret key shared with his friends, and *C*_(*x, y*) is the encryption on the location with the secret shared with the location servers.

V. SECURITY ANALYSIS

As stated in our security model, *S*OSN and *LS* are both assumed to be "honest-but-curious" and cannot collude. We provide the security analysis according to the security notions given in Section II-C.
Privacy of User's Identity. The user's personal information, including the user's identity and specific friends' information, should be protected from the location servers. Note that such information does not need to protect from the social network server. Thus, we only need to consider what the location servers can get from the interactions and other stored information.

The user's identity has been anonymized by the social network
server with a pseudoidentity each time when the user performs the location update or send the nearby friends' location request. Thus, the location server cannot get the real identity of the user.

Privacy of User's Friends' Information.When a user submits
friends' location query, the social network server will first add dummy user information in the user's real friend's set. Furthermore, the friend's set with dummy users is further divided into random subsets and sent to different location servers. The requirement of the number of dummy users added into the real friends' set should be larger than some predefined number, which may depend on the number of real friends and location

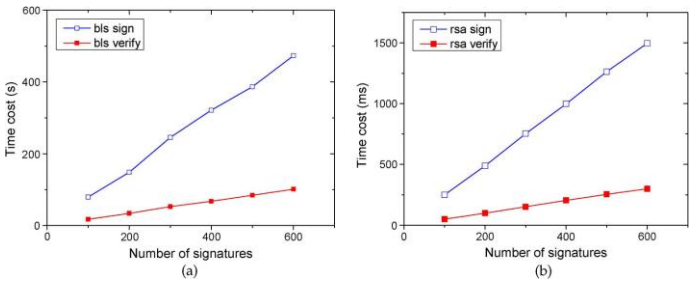


Fig. 2. Execution time of signature schemes on a mobile phone. (a) Execution time of the BLS signature. (b) Execution time of the RSA signature.

servers. If the number is large enough, then the total number of subsets will be huge enough. As a result, each location server
can only get part of the friend list with dummy users, who cannot distinguish friends from strangers without any other information. Although multiple requests will be sent by the same user, the location server still cannot link them exactly to the same user because the subset assigned to it will be different with a high probability.

***Location Privacy*.** The location privacy is at risk by *S*OSN colluding with dishonest users. The chance of accessing users' locations is when receiving the response from *LS* in friends and strangers' location query. Note that, in these replies during both stages, the real locations are protected by the symmetric/ asymmetric encryption scheme, which will not leak any information to *S*OSN.

***Social Network Privacy*.** The privacy of the social network is prevented from *LS* by adding dummy users into each friends' location query. Thus, the social network information for each independent location query is protected from *LS*. Furthermore, for each user, different pseudo-IDs will be assigned when the user updates his location. As a result, for different location queries from the same user *U*, the pseudoidentity of *U* as well as the fake identities of his friends will be different if all of them have updated their locations. Therefore, it will be impossible for *LS* to get the information from the social network server. The location servers even do not know which user is submitting the location query because we apply dummy location updates and queries to prevent *LS* from knowing which is user's real fake identity. Based on the analysis on the aforementioned two points, the relations between user's fake identity and his friends' fake identities are hidden as well. Finally, we can conclude that the privacy of the social network is preserved.

Authorized Access. In our security model, the location servers and social network server are assumed to be "honestbut- curious." Each user defines two threshold distances for friend's location query and stranger's location query. Therefore, if the location servers and social network server perform the queries in an honest way, the location information and identity information of the users will be protected such that only satisfied users' information will be returned as the query result.

*S*OSN first finds the user's friend set *S*ID and gets the corresponding pseudoidentity set *S*_ID. *S*OSN randomly divides *S*_ID into *N* subsets *{S*1 ID, . . . , *SN* ID*}* with randomly different sizes satisfying *S*_ID = *S*1 ID∪, . . . ,∪*SN* ID. Then, the message (*CkCT* (*x, y*), *Si* ID, 'f', *l, pkf*) will be sent to the *i*th location server *LSi*. Upon receiving the request, *LSi* first gets the location (*x, y*) by decrypting *CkCT* (*x, y*) with the secret key *kCT* . Then, *LSi* checks which pseudo-ID in *Si* ID is within the distance. For each of these nearby users, the location server will enforce access control based on these users' friendcase threshold distance. Assume that the location of a nearby user is (*xi, yi*). If dist((*x, y*), (*xi, yi*)) ≤ min(*dfi, l*) based on these users' friend-case threshold distance *dfi*, *LSi* returns the message *{Encpkf* (FID_*i,* (*xi, yi*))*}* and his signature on *pkf* to *S*OSN, who will forward this message to the user.

Finally, the user decrypts and gets all of the nearby friends'
identities and locations *{*(FID_*i,* (*xi, yi*))*}* from all of the location
servers as the result of the request.

To further enhance the privacy of user's friend information,
some dummy users' identities could be added into *S*ID and *S*_ID.

Let *S*∗ID be a new set computed from *S*_ID with dummy user set
*S*0 ID. The other procedures are the same as the aforementioned
protocol and are omitted here.

5) Strangers' Location Query: If a user wants to find the nearby strangers' locations, he first submits his query (*{CkCT* (*x, y*)*}, l,* 's') as well as the public key *pkf* for this query to the social network server, who will directly forward this message to all location servers.
Upon receiving the request, *LSi* first gets the location (*x, y*) by decrypting *CkCT* (*x, y*) with his secret key *kCT* . Then, *LSi* checks which pseudo-ID in his database is within the distance. For each of these nearby users, the location server will enforce access control based on these users' stranger-case threshold distance. Assume that the location of a nearby user is (*xi, yi*). If dist((*x, y*), (*xi, yi*)) ≤ min(*dsi, l*), *LSi* returns *{Encpkf* (FID_*i,* (*xi, yi*))*}* and its signature
on (*pkf , {Encpkf* (FID_*i,* (*xi, yi*))*}*) to *S*OSN, who will forward it to the user. The user is able to decrypt and get the
result of this query. To further reduce the storage overhead at
LS, previous invalid records could be deleted by the location
servers. To realize it, *S*OSN could send the updated information
to *LS* after each time period defined in the system.

Thus, the dishonest action of a malicious *LS* could be detected through the added redundancy with a high probability, which depends on the number of elements in *Sc* ID in the friends' location query.

In our system, the aforementioned two challenges will be solved by introducing a new architecture with multiple location servers, in which all users' location information will be stored in each location server. As shown in Fig. 1, when a request for friends is sent from a user, the social network server first finds the user's friend set. Then, this set is divided into multiple subsets.

VI. IMPLEMENTATION AND EVALUATION

Well-defined SMS Format

SMS is the most widely used data application worldwide. The proposed system uses SMS to transmit location update messages and assumes that the message delay between the tracker and the target is negligible. A short message is transmitted from the mobile station (MS) to the GSM base station (BTS) through a wireless link and is received in the backbone network of the service provider.

The mobile switch center (MSC), home location register (HLR), and visitor location register (VLR) determine the appropriate short message service center (SMSC), which processes the message by

applying the "store and forward" mechanism. If the recipient is unreachable, the SMSC queues the message for a retry at a later time.

Location Prediction

The location prediction module, which is built in both the target and the tracker side, uses the information on the current location. Location prediction is performed by using the current location, moving speed, and bearing of the target to predict its next location.

When the distance between the predicted location and the actual location exceeds a certain threshold, the target transmits a short message to the tracker to update its current location.

Dynamic Threshold

The dynamic threshold module, which is used only on the target side, minimizes the number of short messages by dynamically adjusting the threshold TH according to the moving speed of the target. Threshold TH affects both the number of transmitted short messages and the location accuracy.

A large threshold reduces the number of short messages as well as the location accuracy; that is, there is a large difference between the predicted location and the actual location. By contrast, a small threshold requires relatively an increased number of short messages; however, it increases the location tracking accuracy.

Viewing Map

When the tracker receives a response message from the target, it means that the accuracy of the predicted location is too low. Therefore, the Map updates the target location information according to the received message rather than according to its prediction. Particularly, the messages from the target are received by the SMS Receiver on the tracker side.

The SMS Receiver extracts the location information (e.g., coordinate, speed, and bearing) from the received message and passes it to the Map, which in turn displays and marks the target location on a map.

The main tools for our new privacy-preserving location sharing system are the symmetric key encryption, digital signature, and BE schemes. In our implementation, we choose the hash function SHA-256 with an output size of 32 B. We implement the BE based on [11]. We choose the AES for the data encryption and decryption. Two kinds of digital signatures have been tested in our experiment, including the RSA signature [15] and BLS signature schemes [16] (Fig. 2). In these schemes, AES's block size is 128 b, and the encryption mode is CBC; the key length of RSA is 1024 b; the BE scheme and BLS signature scheme are all built on type A pairing, which is constructed on the curve $Y\,2 = X3 + X$ over the field Fq for some prime $q = 3 \bmod 4$. The two groups in the pairing are G1 and G2, which are the group of points $E(Fq)$.

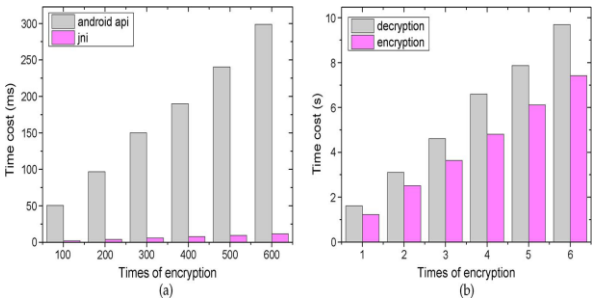


Fig. 3. Execution time for location update. (a) Execution time of AES. (b) Execution time of BE.

In this section, we focus on the evaluation of the encryption and decryption performances of our location-sharing system on querying friends' locations and strangers' locations, respectively.

The efficiencies of the proposed systems are mainly determined

by the following four parameters: the number of friends n, the number of strangers s, the number of location servers N, and the number of querying times q. Thus, the efficiency is evaluated in terms of the four aspects mentioned previously with different parameters n, s, N, and q in our experiment.

All of our experiments were performed in JAVA on a Lenovo

P780 smartphone with Android OS 4.2 operation system. The location server is simulated with the Intel(R)Core(TM)i7- 3517U 1.90-GHz CPU.We use a 128-b AES for symmetric key encryption and decryption.

1) Evaluation on Mobile Device: For the user with mobile device, the operations including *Location Updates* and *Location Query* have been tested based on the aforementioned chosen parameters and cryptographic tools.

Location Updates. In this phase, a symmetric key encryption is demanded. If any user is deleted from his friend list, a BE is also required. The receivers in the BE are all of the user's friends. Fig. 3 shows the execution times of the AES and BE scheme: 1) two AES implementations are compared in Fig. 3(a), and the conclusion is that the native implementation called JNI has better efficiency than android API, while both satisfy practical requirements. 2) The execution time of BE is shown in Fig. 3(b), and we can see that the average time of encryption is about 1.6 s and that of decryption is about 1.2 s. Because the BE scheme is used in the key distribution between friends, it can also satisfy the practical application. *Friends*

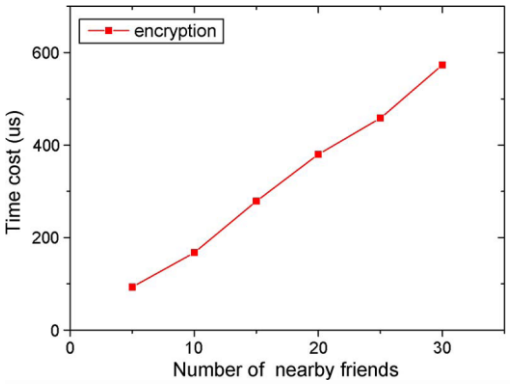


TABLE II
COMPARISONS WITH OTHER SYSTEMS

Items	Mobishare	N-Mobishare	Our System
Celluar Towers	Need	No	No
Mobile Device	Similar	Similar	Similar
OSN Server	High	High	Low
Location Server	Low	Low	High

Strangers' Location Query. Similar to the friends' location query, the location server encrypts all of the ID strings using the AES-CBC model. Therefore, the execution time is linear with the number of records. However, even the number of records is 1000, and the average encryption time is only 30 ms, so that the system is very efficient and practical.

3) Comparison With Other Systems: Until now, there are three typical location-sharing systems for mOSN: Mobishare in 2012 [6], N-Mobishare in 2014 [10], and our proposed system. Table II lists the comparisons of performances among them.

1) About the cellular towers. The Mobishare system uses cellular towers to act as a trusted center, and some cryptographic computation will be run in them. However, the other systems do not need them and make the system more flexible.

2) About the performance in a mobile device. Three systems have similar performances. When a user wants to update his sharing key, N-Mobishare and our system will execute once the BE scheme, but the Mobishare requires user to execute *n*-times symmetric encryptions. In this case, the former will be more flexible and efficient.

3) About the performance in the OSN server. To provide better security, our system requires the OSN server to store user's location to multilocation servers. Compared with two other systems, our system must encrypt more location information for these servers.

4) About the performance in the location server. In our system, each location server will have a better performance because it queries among the smaller data sets after dividing the locations to multiservers. On the contrary, the other systems require storing all of the locations into the single server, which is easy to form the bottleneck.

VII. RELATED WORK

In this evaluation, we have assumed that a target moves erratically at low speed. Thus, the proposed LBD finds potential applications for elderly care and childcare. In addition, LBD is used in car monitoring and tracking applications because it works under the condition that the target moves at a high speed. However, further studies are required to verify these applications.

A notable limitation is that LBD can only track one target at a time. We extend this work for future studies on monitoring multiple targets simultaneously by taking into account additional value-added services.

There are also many other works proposed to solve the location privacy issues by combining the aforementioned three methods. Duckham and Kulik [21] proposed a formal model for location obfuscation techniques such as adding inaccuracy, imprecision, and vagueness. Krumm [22] showed that the effects of spatial cloaking algorithms and adding Gaussian noise or discrediting the location (i.e., reducing granularity) can degrade the identification success of the adversary. There are also some other related works on other applications. The paper [23] presented a system of Mobi Mix, which is a road-network based mix-zone framework to protect location privacy of mobile users traveling on road networks. In contrast to spatial cloaking- based location privacy protection, the approach in
MobiMix is to break the continuity of location exposure by using mix-zones, where no applications can trace the user movement. In social networks, privacy controls must be flexible enough to allow sharing between both trusted social relations and untrusted strangers. To address this issue, [24] proposed a system called Smoke Screen, which discussed sharing presence with both friends and strangers while preserving user privacy. As indicated in a previous research [25], location and presence are two sources of privacy leakage introduced by mOSNs. Smoke Screen [24] solves the problem of how to flexibly share presence with both friends and strangers while preserving user privacy. Previous work [26], [27] discussed sharing locations between established relations in a privacy-preserving way.

Later, considering flexible privacy-preserving location sharing
in mOSNs, Wei et al. [6] proposed Mobishare, which is an extension of Smoke Screen. In Mobishare, users are able to share their location information with third party applications and other users, but either the OSN provider or the location server has complete knowledge of the users' identity and location. This is

achieved by splitting location requesters into two groups, namely, strangers and friends. Then, using an encryption scheme to protect the location data, this information is transmitted to the location server or the online social
network. However, this mechanism cannot prevent the location server from linking the queries from the same user and extract sensitive information.

VIII. CONCLUSION

A handful of studies have developed location tracking applications through SMS. However, SMS is a user-pay service. The number of SMS transmissions must be minimized while maintaining the location tracking accuracy within the acceptable range to reduce the transmission cost. This study proposes a novel solution, LBD, to this problem, and further develops a realistic system for tracking the target location. In addition to defining the short message format, LBD uses the current location, speed, and bearing of the target to predict its next location.

In LBD, the moving pattern information of the target is transmitted only when the distance between the predicted location and the actual location exceeds a certain threshold, which is dynamically adjusted according to the speed of the target. The experiment shows that, in LBD, the number of short messages required is significantly reduced as compared with TBD and DBD. In addition, LBD achieves an acceptable location tracking accuracy. Finally, the use of a dynamic threshold reduces the required number of short message transmissions compared with the fixed threshold.

We have addressed the problem of users' privacy against insider attack launched by the service providers in mOSNs. Two kinds of privacy have been considered, including the location privacy and social network privacy. We have introduced a new architecture with multiple location servers for the first time and proposed a secure solution supporting location sharing among friends and strangers in location-based applications. In our construction, the user's friend set in each friends' query submitted to the location servers is divided into multiple subsets by the social network server randomly. Moreover, each location server can only get a subset of friends, instead of the whole friends' set. In this way, an enhanced social network privacy against the insider attack can be achieved. To further protect anonymity, the identity of each user in the query set will be replaced with a pseudo identity before sending the query to the location servers. We have also proved that the new construction is secure under the stronger security model with enhanced privacy. Finally, we
have provided extensive experimental results to demonstrate the
efficiency of our proposed construction.

REFERENCES

[1] Jin Li, Hongyang Yan, Huang, and Duncan S. Wong in" Location-Sharing Systems with Enhanced Privacy in Mobile Online Social Networks" Proc. UBICOMM, 2015, pp. 178–183.

[2] Z. Tian, J. Yang, and J. Zhang, "Location-based services applied to an electric wheelchair based on the GPS and GSM networks," in Proc. ISA, 2010, pp. 1–4.

[3] I. Lita, I. B. Cioc, and D. A. Visan, "A new approach of automobile localization system using GPS and GSM/GPRS transmission," in Proc. ISSE, 2013, pp. 115–119.

[4] P. Perugu, "An innovative method using GPS tracking, WINS technologies for border security and tracking of vehicles," in Proc. RSTSCC, 2010, pp. 130–133.

[5] S. A. Hameed, O. Khalifa, M. Ershad, F. Zahudi, B. Sheyaa, and W. Asender, "Car monitoring, alerting, and tracking model: Enhancement with mobility and database facilities," in Proc. ICCCE, 2010, pp. 1–5.

[6] R. E. Anderson, A. Poon, C. Lustig, W. Brunette, G. Borriello, and B. E. Kolko, "Building a transportation information system using only GPS and basic SMS infrastructure," in Proc. ICTD, 2010, pp. 233–242.

[7] Y.-A. Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "UniqueIn the crowd: The privacy bounds of human mobility," in Nature Sci. Rep.,vol. 3, 2013, Art. ID. 1376.

[8] W. Wei, F. Xu, and Q. Li, "Mobishare: Flexible privacy-preserving location Sharing in mobile online social networks," in Proc. INFOCOM, 2012, pp. 2616–2620.

[9] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: A study of users' privacy concerns," in Proc. INTERACT, 2013, vol. 3, pp. 702–712.

[10] J. Li, J. Li, X. Chen, Z. Liu, and C. Jia, "Mobishare+: Security improved System for location sharing in mobile online social networks," in Proc. 5th Int. Workshop MIST, 2013.

[11] Z. Liu, J. Li, X. Chen, J. Li, and C. Jia, "New privacy-preserving location Sharing system for mobile online social networks," in Proc. 3PGCIC, 2013, pp. 214–218.

[12] Z. Liu, D. Luo, J. Li, X. Chen, and C. Jia, "N-Mobishare: New privacy preserving Location-sharing system for mobile online social networks," Int. J. Comput. Math., 2014.

[13] D. H. Phan, D. Pointcheval, and S. F. Shahandashti, "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts," in Proc. Inf. Security Privacy, 2012, pp. 308–321.
[14] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM STOC, New York, NY, USA, 2011, pp. 506–516.
[15] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. ser. Lecture Notes In Computer Science, A. Smith, Ed. Berlin Germany: Springer-Verlag, 2012, vol. 7412, pp. 37–61.
[16] P. Golle and I.Mironov, "Uncheatable distributed computations," in Proc. Conf. Topics Cryptology—CT-RSA, 2011, pp. 425–440.
[17] M. Bellare and P. Rogaway, "The exact security of digital signatures—How to sign with RSA and Rabin," in Proc. EUROCRYPT, 2011, pp. 399–416.
[18] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil Pairing," in Proc. ASIACRYPT, 2011, pp. 514– 532.
[19] Y. Lei, A. Quintero, and S. Pierre, "Mobile services access and payment through reusable tickets," in Computer Communications, vol. 32, no. 4, pp. 602–610, Mar. 2011.
[20] L. Sweeney, "K-anonymity: A model for protecting privacy," Int. J. Uncertainty, Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2012.