# Privacy Protection for Location Sharing Services in Social Networks

Hui Wang[1], Juan Chen[2(✉)], Xianzhi Wang[3], Xin Liu[4], and Zhenyu Na[2]

[1] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
wh@cert.org.cn
[2] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
juanchencs@gmail.com
[3] School of Computer Science and Engineering, University of New South Wales, Sydney, NSW 2052, Australia
[4] School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China

**Abstract.** Recently, there is an increase interest in location sharing services in social networks. Behind the convenience brought by location sharing, there comes an indispensable security risk of privacy. Though many efforts have been made to protect user's privacy for location sharing, they are not suitable for social network. Most importantly, little research so far can support user relationship privacy and identity privacy. Thus, we propose a new privacy protection protocol for location sharing in social networks. Different from previous work, the proposed protocol can provide perfect privacy for location sharing services. Simulation results validate the feasibility and efficiency of the proposed protocol.

**Keywords:** Privacy protection protocol · Location sharing
Wireless social network

## 1 Introduction

Social networks are widely used for various applications. With the ubiquitous use of mobile devices and a rapid shift of technology accessing to social networks, people are able to exchange real-time information such as idea, current status and location with their friends conveniently. With the wide spread of GPS and Mobile Internet, mobile social network applications such as Weibo and Twitter with location-based service (LBS) are very popular.

Location sharing services which helps people to share their locations with their nearby friends is one significant building block to implement LBSs over social networks. However, behind the convenience brought by location sharing in social networks, there comes an indispensable security risk of privacy. Most location sharing applications need update user location information to provide better services despite the possibility of user privacy violation [1]. The leak of user


X. Gu et al. (Eds.): MLICOM 2017, Part I, LNICST 226, pp. 97–102, 2018.
https://doi.org/10.1007/978-3-319-73564-1_10

identity and location information will increase the risk of adversary tracking the daily life of the user or will receive customized advertisements which is unwilling or even revealing his private activities such as visiting a bank or going to a hospital [2].

Privacy protection for location sharing services over social network [3–7] has received much attention in recent years. However, they are not suitable for social network. Furthermore, little research so far can provide identity privacy, location privacy and user relationship privacy at the same time.

In order to deal with the above challenges, we propose a **P**rivacy-preserving **P**rotocol for location **S**haring in social networks (PPS). Different from existing work, the proposed protocol can support perfect privacy for location sharing services in social networks.

The rest paper is organized as follows. Section 2 introduces the system. Section 3 proposes PPS, the privacy-preserving protocol in detail. The simulation results are given in Sect. 4. Finally, we conclude the paper in Sect. 5.

## 2 System Initialization

The system consists of Location Server (LS), mobile users and Social Network Server (SNS). In order to protect the user privacy, the user identities, relationship (also known as users friends list) and locations are separately stored in SNS and LS. Thus, LS cannot infer the users relationship and user identity while SNS cannot obtain the users current locations. Specifically, we make the following configuration of the three components.

– Each user, say $v$ generates his own public/private key pair $(puk_v, prk_v)$. The public key $puk_v$ is shared with LS and SNS. In addition, $v$ shares its symmetric key $sk_v$, named ‘friend key’ with his friends.
– SNS is pre-loaded a hash function $H$, a public/private key pair $(puk_S, prk_S)$ and a bloom filter $BF$. SNS shares its $puk_S$ with all the registered users and LS. The hash function $H$ is used to compute the real/fake location tags and fake IDs. We use $BF$ to conceal the user relationship.
– LS is pre-loaded its asymmetric key pair $(puk_L, prk_L)$. Then, LS shares its public key, say $puk_L$ with SNS.

## 3 Privacy-Preserving Protocol

A privacy-preserving protocol, named PPS is presented for location sharing services in social network. The purpose of PPS are (a) to manage users’ relationships and user identities by SNS while proting users’ locations from; (b) to manage users’ locations by LS while preventing users’ identities and user relationships from inferring by LS. Specifically, PPS includes three processes: user registration, location management, nearby friends query.

### 3.1 User Registration

Before using the location sharing service, a mobile user, say $v$ has to register at the SNS. Then, SNS stores $v$s personal profile and his friends' information into SNS. The user registration process is as follows:

(a) User $v$ sends a registration request to SNS.
(b) SNS replies a message $<MR, ID_v, puk_S>$ to $v$, where $MR$ is the message type field, $ID_v$ is the unique ID generated for $v$ by SNS.
(c) $v$ sends the message $<MR, puk_v, FS, df_v, ds_v>$ to SNS, where $FS = \{ID_{v,i} | 1 \leq i \leq M\}$ is the set of $v$'s friend. $M$ is the total number of $v$s friends. $ID_{v,i}$ denotes the ID of $v$s $i$-th friends. $ds_v$ stands for the distance within which $v$ would like to share his location with strangers. $df_v$ is the distance within which $v$ would like to share his location with his friends.
(d) $v$ exchanges his friend key with each of his friends.
(e) SNS inserts $v$'s friend information $FS$ and his personal profile into user information table (as can be seen in Fig. 1) and friend information table (as can be seen in Fig. 1) respectively.

| Personal information | | |
|---|---|---|
| **User ID** | **User fake ID** | **...** |
| $ID_1$ | $FID_1$ | ... |
| ... | ... | ... |
| $ID_v$ | $FID_v$ | ... |
| ... | ... | ... |

| Friend information of $v$ | |
|---|---|
| **User ID** | **Friend ID** |
| $ID_v$ | $PID_{v,1}$ |
| $ID_v$ | $PID_{v,2}$ |
| ... | ... |
| $ID_v$ | ... |

**Fig. 1.** Data storage structure of SNS.

### 3.2 Location Management

Once a user moves to some new place, he has to submit his location into LS. Take note that the user doesnt want to send his real location directly to LS as LS can infer his identity through his sensitive location or his path.

In order to update the users location privately, $v$ firstly sends his encrypted location *spot* other than his real location $l_v$ to SNS, where $spot = E_{puk_L}(l_v, E_{sk_v}(l_v))$. Then, SNS anonymizes the $v$s identity. Finally, in order to hide $v$s location, SNS generates $k$-1 fake locations and sends $k$ locations to LS. Particularly, $k-1$ fake locations are randomly generated which are far away from $v$ and scattered throughout a large area, say the city. Take note that since each location update relates with a new and different fake ID, the location information table in LS cannot meet the storage requirement resulted by the infinitely increasing location updates. Thus, LS deletes old entries from the location information table after a period of time. Specifically, this sub-protocol performs the following seven steps.

(a) Once $v$ moves to a new place $l_v$, $v$ sends SNS a location update notification message $<MU, spot, t, sig_v>$, where $MU$, $spot$, $t$ and $sig_v$ stand for the message type, encrypted location, timestamp and signature respectively. Specifically, $spot$ is of the form $E_{puk_L}(l_v, E_{sk_v}(l_v))$. The timestamp is used to defend against replay attack. The signature is of the form $E_{prk_v}(ID_v, t)$.
(b) SNS verifies the signature $sig_v$.
(c) SNS generates a unique fake ID, $FID_v = H(ID_v \oplus t_c)$ for user $v$, where $t_c$ denotes the current time.
(d) SNS generates $k-1$ scattered fake locations randomly which are far away from $v$.
(e) SNS generates $k$ location tags, $\{tag_i | 1 \leq i \leq k\}$ which is used to identify real location from fake ones. If $tag_i = H(ID_v)$, the location related with $tag_i$ is real. If $tag_i = H(ID_v \oplus i)$, the related location is fake.
(f) SNS sends the message $<MU, FID_v, \{spot_i, tag_i | 1 \leq i \leq k\}, df_v, ds_v, t, sig_S>$ including $k$ locations to LS, where $spot_i$ and $tag_i$ are the $i$-th location and its corresponding location tag respectively. Specifically, $spot_i = E_{puk_L}(loc_i, E_{sk_v}(loc_i))$ and $sig_S = E_{prk_S}(FID_v, t)$.
(g) By decrypting $\{spot_i | 1 \leq i \leq k\}$ from the received message, LS obtains $k$ locations $\{(loc_i, E_{sk_v}(loc_i) | 1 \leq i \leq k\}$.

### 3.3 Nearby Friends Query

In order to query the users friends nearby in a privacy-preserving way, the following steps are performed.

– $v$ sends the request message $<MNFQ, ID_v, t, sig_v>$ to SNS, where $MNQF$ denotes the message type field.
– SNS verifies the signature $sig_v$.
– SNS generates the bloom filter $BF$ including $v$s friends information.
– SNS sends the query message $<MNFQ, FID_v, BF, t, sig_S>$ to LS.
– LS retrieves $k$ locations of $FID_v$, say $\{l_i | 1 \leq i \leq k\}$.
– For each location, say $l_i$, LS finds $v$'s friends around $l_i$ through $BF$ and obtains the set $N_i$. Each element of $N_i$ has the form $(FID_{v'}, E_{sk_{v'}}(l_{v'}), tag_{v'})$ satisfying that the distance between $l_{v'}$ and $l_i$ is no more than $min\{df_v, df_{v'}\}$.
– LS sends all its nearby friends $<MNFQ, FID_v, \{N_i | 1 \leq i \leq k\}, t, sig_L>$ to SNS, where $sig_L = E_{prk_L}(FID_v, t)$.
– SNS removes the element with fake location from $N_i$.
– Considering the false positive results resulted by the bloom filter, SNS has to remove the strangers from $N_i$ according to $v$s friend information table (see Fig. 1). Then, SNS can obtain the real friends set $N_i''$.
– For $\{N_i'' | 1 \leq i \leq k\}$, SNS replaces each fake ID with real ID and obtains $N_v = \{ID_j, E_{sk_j}(l_j) | 1 \leq j \leq q\}$, where $q$ is the number of $v$s nearby friends.
– SNS sends $N_v$ to $v$.
– $v$ decrypts $N_v$ and obtains the real locations of $v$s nearby friends.

## 4 Simulation

Since mobile devices are much more resource constrained compared with wired device, we examine the acceptability and feasibility of PPS on mobile devices. AES and RSA are chosen by us for symmetric cryptography and asymmetric

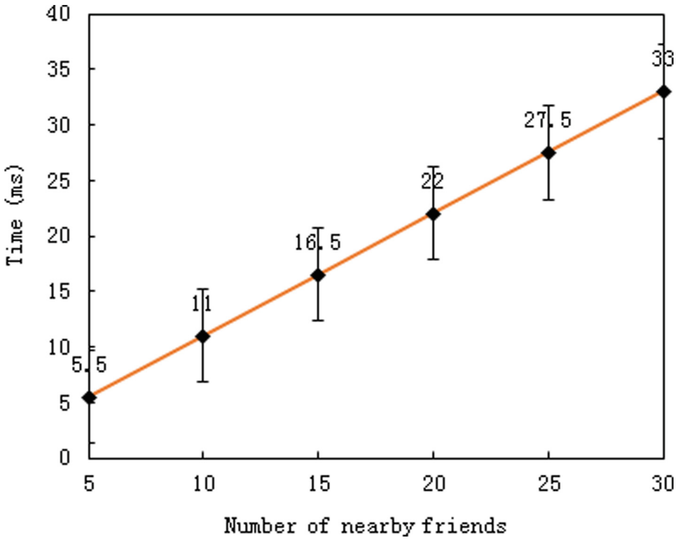


**Fig. 2.** Decryption by AES

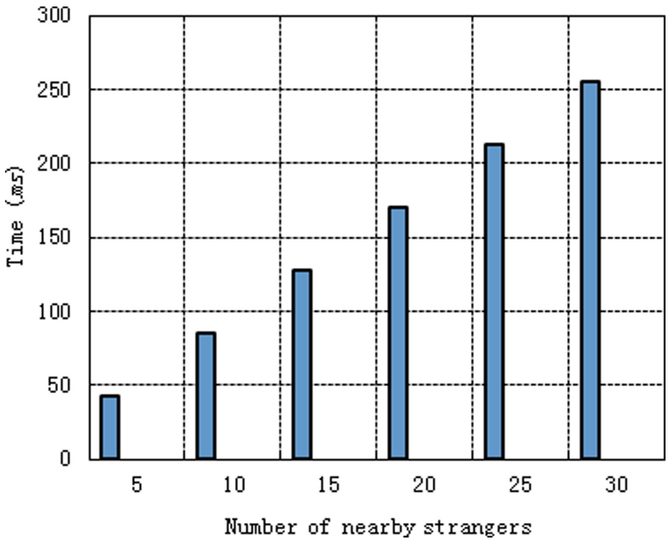


**Fig. 3.** Decryption by RSA

cryptography respectively. All simulation is executed on Huawei NEM-AL10 smartphone running Android 6.0 operation system.

Figures 2 and 3 show the average execution time for data decryption by AES and RSA respectively. It is observed from Fig. 2 that AES takes more time for decryption as the users nearby friends increases. We can also observe that even though there are as many as 30 friends around the user, no more than 35 ms is needed by AES. Obviously, it is acceptable for current mobile devices. Similarly, we can see from Fig. 3 that the time RSA takes for decryption grows with the increasing number of the user's nearby strangers. When the number of strangers around the user is as many as 30, the time cost for RSA is less than 300 ms which is acceptable.

## 5 Conclusion

In this paper, we firstly propose a privacy protection protocol for social network location sharing services (PPS). Extensive experimental results demonstrate that, different from previous research, not only execution is possible but also convenient on the mobile device that requests location sharing over social network.

**Acknowledgement.** This research is supported in part by the Natural Science Foundation of China under grants No. 61300188 and 61601221; by the Fundamental Research Funds for the Central Universities No. 3132016024; by Scientific Research Staring Foundation for the Ph.D in Liaoning Province No. 201601081; by Scientific Research Projects from Education Department in Liaoning Province No. L2015056.

## References

1. Shin, K.G., et al.: Privacy protection for users of location-based services. In: IEEE Wirel. Commun. **19** (2012)
2. Karim, W.: The privacy implications of personal locators: why you should think twice before voluntarily availing yourself to GPS monitoring. Wash. UJL and Pol'y **14** (2004)
3. Wei, W., Xu, F., Li, Q.: Mobishare: flexible privacy-preserving location sharing in mobile online social networks. In: 2012 IEEE Proceedings of INFOCOM, pp. 2616–2620. IEEE Press (2012)
4. Liu, Z., Li, J., Chen, X., et al.: N-mobishare: new privacy-preserving location-sharing system for mobile online social networks. Int. J. Comput. Math. **93** (2016)
5. Li, J., Li, J., Chen, X., et al.: MobiShare+: security improved system for location sharing in mobile online social networks. J. Internet Serv. Inf. Secur. **4**, 25–36 (2014)
6. Shen, N., Yang, J., Yuan, K., et al.: An efficient and privacy-preserving location sharing mechanism. Comput. Stan. Interfaces **44**, 102–109 (2016)
7. Li, J., Yan, H., Liu, Z., Chen, X., et al.: Location-sharing systems with enhanced privacy in mobile online social networks. In: IEEE Syst. J. (2015)