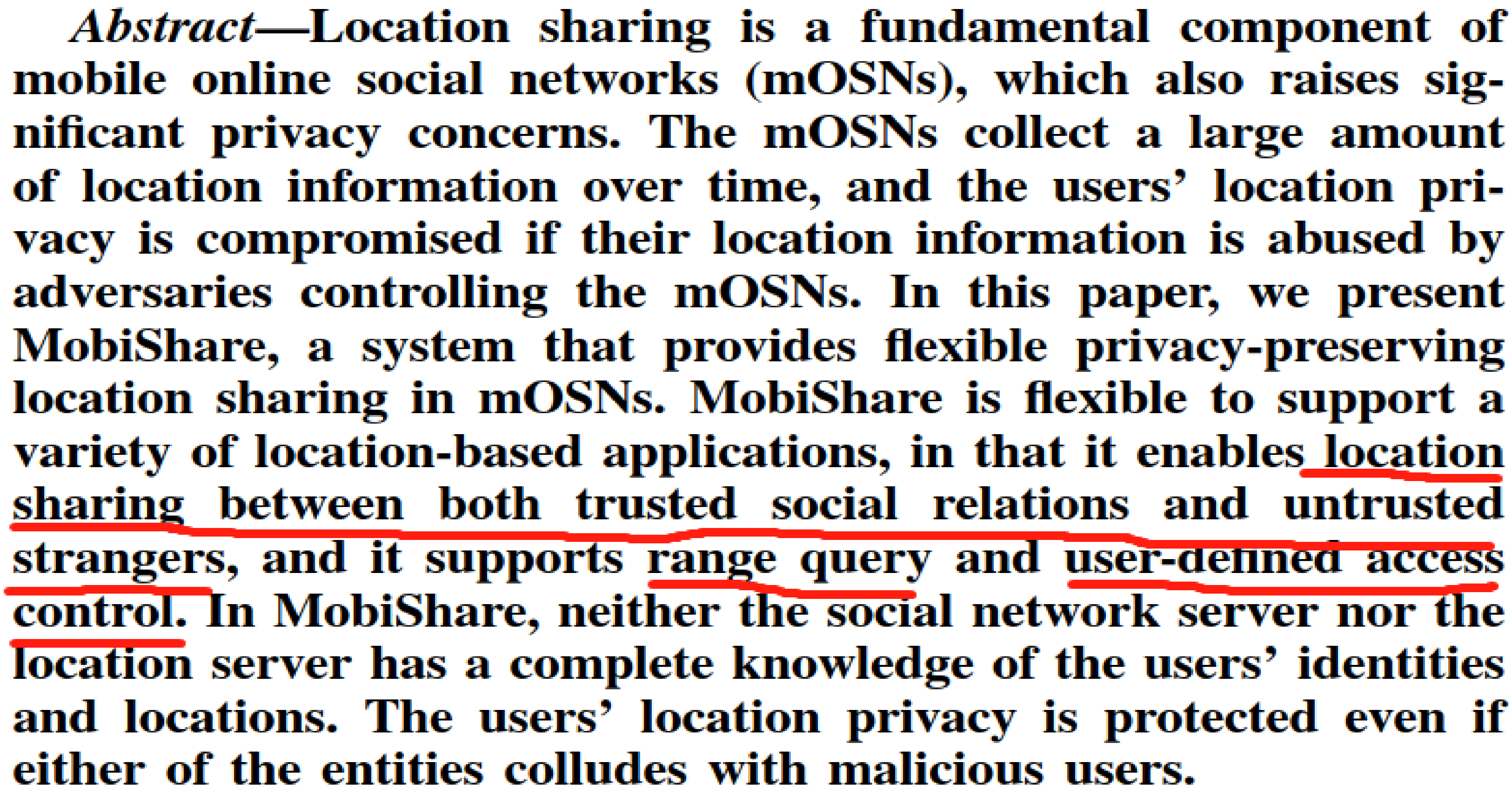
# Abstract

A simple review of privacy-preserving location sharing scheme over mobile online social network.

# MobiShare: Flexible Privacy-Preserving Location Sharing in Mobile Online Social Networks

Wei Wei, Fengyuan Xu, Qun Li
Computer Science, The College of William and Mary
{wwei, fxu, liqun}@cs.wm.edu



*Abstract*—Location sharing is a fundamental component of mobile online social networks (mOSNs), which also raises significant privacy concerns. The mOSNs collect a large amount of location information over time, and the users' location privacy is compromised if their location information is abused by adversaries controlling the mOSNs. In this paper, we present MobiShare, a system that provides flexible privacy-preserving location sharing in mOSNs. MobiShare is flexible to support a variety of location-based applications, in that it enables location sharing between both trusted social relations and untrusted strangers, and it supports range query and user-defined access control. In MobiShare, neither the social network server nor the location server has a complete knowledge of the users' identities and locations. The users' location privacy is protected even if either of the entities colludes with malicious users.

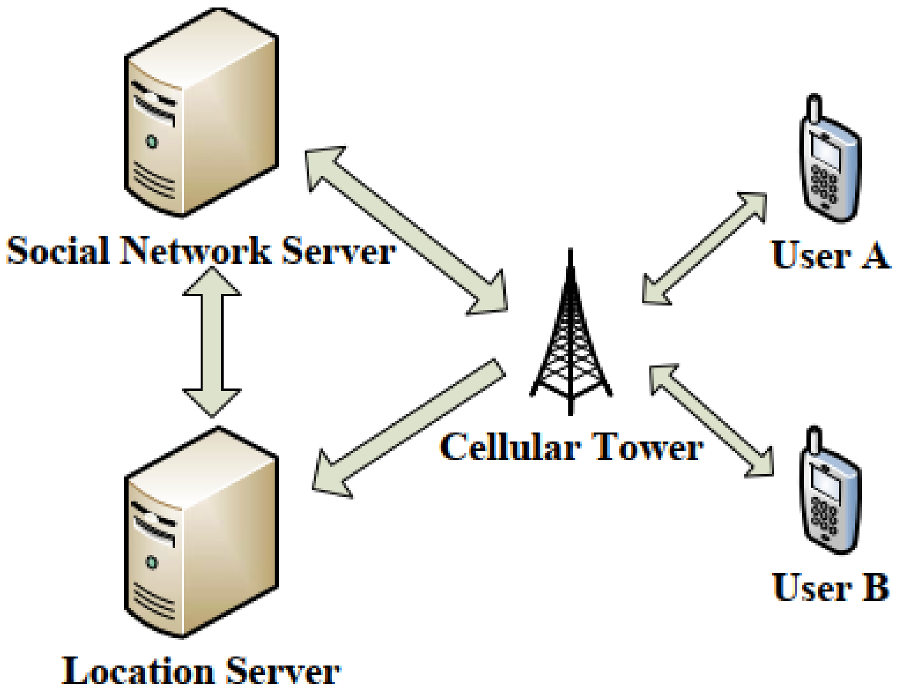


Fig. 1. System architecture

**SNS:** a server of any existing OSN that wants to provide the location-sharing service.

Users' ID and friend lists

**LS:** an untrusted third-part server

Stores anonymized location updates of the users.

symmetric secret key ➡ **CT**

**CT:** symmetric secret key ➡ **LS**

**User:** each user has a unique identifier at the social network server.

a public-private key pair

a symmetric session key ➡ social network friends

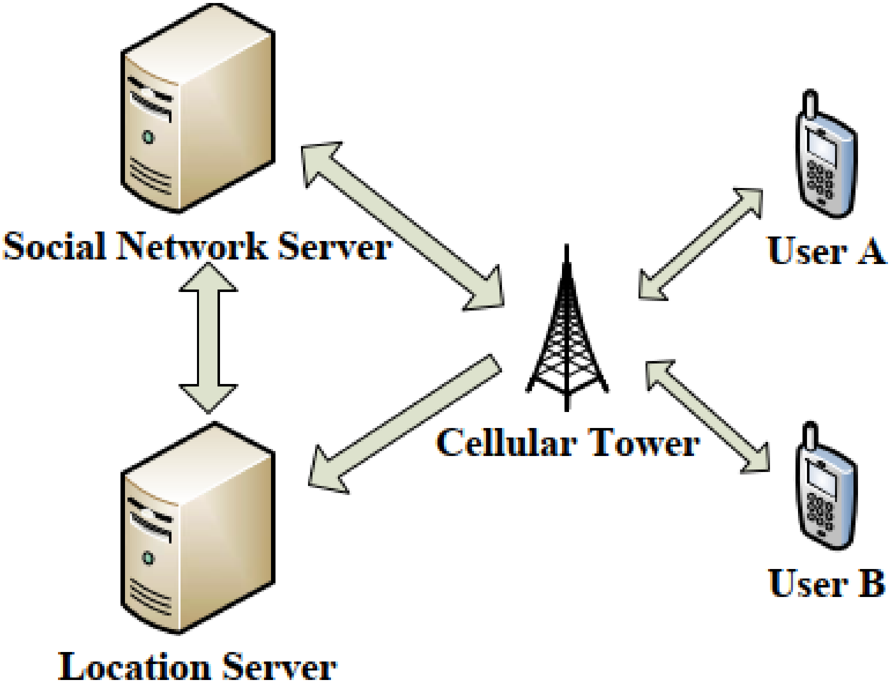


Fig. 1. System architecture

## A. Service Registration (at SNS)

(1) User sent PubKeyA to SNS

(2) Define: access control settings (two threshold distances): dfA and dsA

User A gets $ID_A$

SNS stores $\langle ID_A, PubKey_A, df_A, ds_A \rangle$

## *B. Authentication*

User A → $(ID_A, ts, \underline{Sig_A}(ID_A, ts))$ → CT → SNS

SNS uses $PubKey_A$ to verify A's signature.

↓

verification succeeds

↓

SNS sent $(ID_A, df_A, ds_A)$ → CT → User A

↓

User A → OK CT stores $(ID_A, df_A, ds_A)$

## C. Location Updates

CT perform anonymization → identities cannot be inferred from the anonymized location

pseudonyms dummy location updates.

fake IDs ← a cryptographic hash function, such as SHA-1 and a random salt value

$$fake\ ID_i = SHA(fake\ ID_{i-1} \oplus salt)$$

User A $\xrightarrow{(ID_A,(x,y),Sess_A(x,y))}$ CT $\xrightarrow{k \text{ fake IDs}}$ real location

$k-1$ fake IDs construct dummy location updates.

CT $\xrightarrow{\langle ID_A, FID_A, FID_1, ..., FID_{k-1} \rangle}$ SNS

CT $\xrightarrow{\substack{(FID_A,(x,y),Sess_A(x,y),df_A,ds_A) \\ (FID_i,(x_i,y_i),str_i,df_i,ds_i)}}$ LS

### *D. Querying Friends' Locations*

User A $\xrightarrow{query(ID_A,\ `f',\ `1mi')}$ CT $\xrightarrow{query(ID_A,\ `f',\ `1mi',\ \boxed{SecKey_{Loc}(CID_C, seq))}}$ SNS

SNS $\xrightarrow{query(\boxed{FID_A,}\ `f',\ \boxed{FIDlist,}\ `1mi',\ SecKey_{Loc}(CID_C, seq))}$ LS distance computation

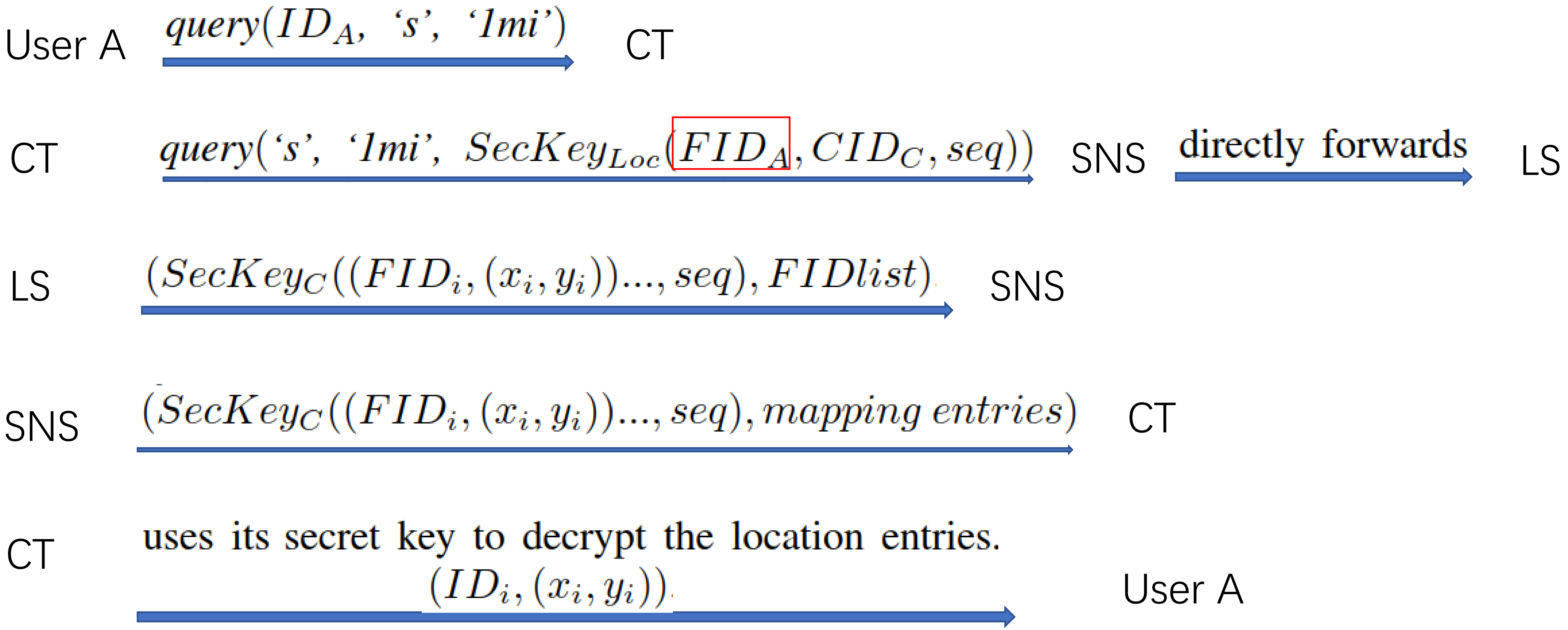
access con-trol enforcement.

LS $\xrightarrow{SecKey_C((FID_i, Sess_i(x_i, y_i))..., seq).}$ SNS

SNS $\xrightarrow{\substack{SecKey_C((FID_i, Sess_i(x_i, y_i))..., seq). \\ \text{a mapping entry for each of A's friends}}}$ CT $\xrightarrow{\substack{\text{replaces fake ID} \\ \text{discarded dummy location}}}$

CT $\xrightarrow{(ID_i, Sess_i(x_i, y_i)).}$ User A $\xrightarrow{\substack{\text{decrypt} \\ \text{get the plaintext locations of the nearby friends.}}}$

### E. Querying Strangers' Locations



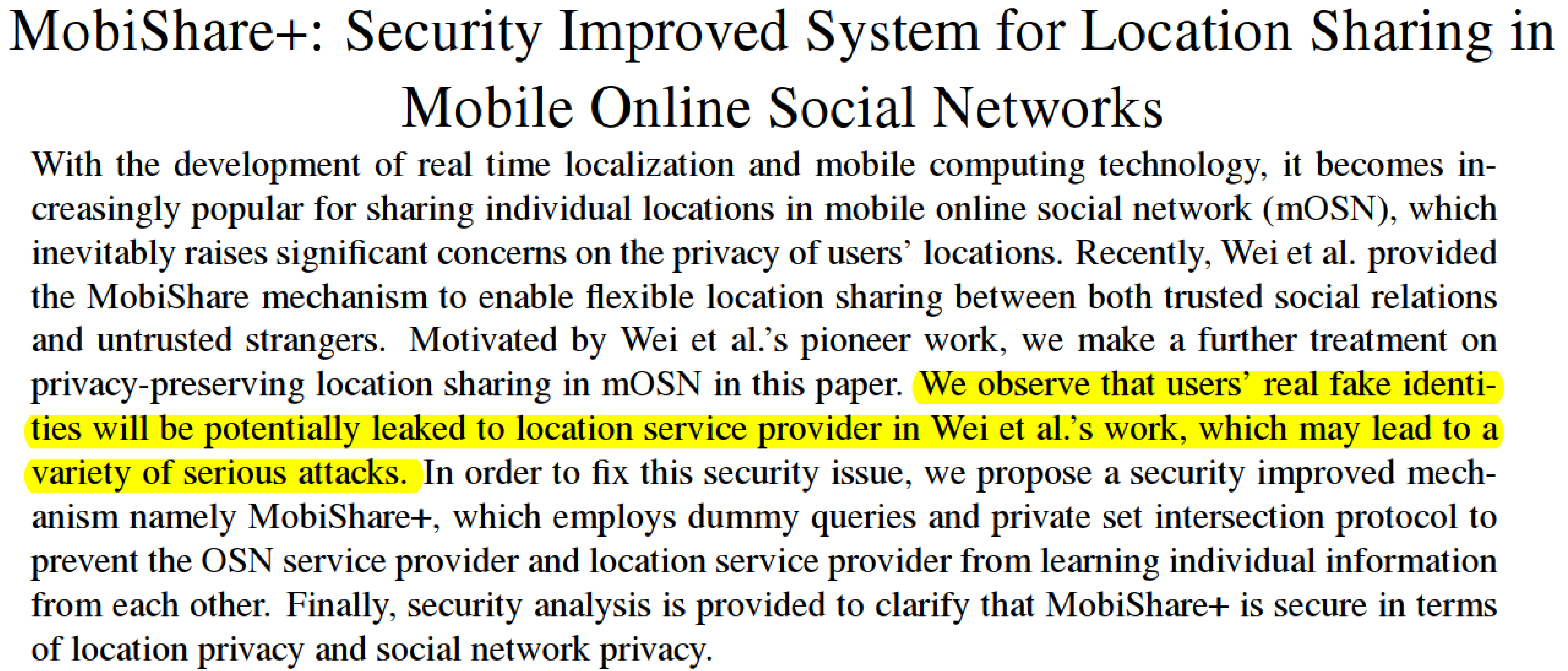
User A $\xrightarrow{query(ID_A,\ \text{‘}s\text{’},\ \text{‘}1mi\text{’})}$ CT

CT $\xrightarrow{query(\text{‘}s\text{’},\ \text{‘}1mi\text{’},\ SecKey_{Loc}(\boxed{FID_A}, CID_C, seq))}$ SNS $\xrightarrow{\text{directly forwards}}$ LS

LS $\xrightarrow{(SecKey_C((FID_i,(x_i,y_i))...,seq),FIDlist)}$ SNS

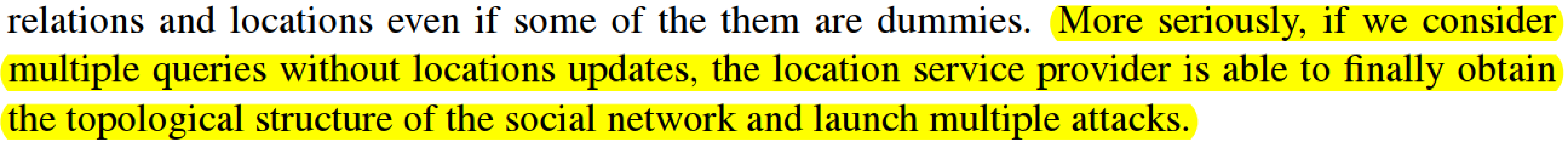
SNS $\xrightarrow{(SecKey_C((FID_i,(x_i,y_i))...,seq),mapping\ entries)}$ CT

CT uses its secret key to decrypt the location entries. $\xrightarrow{(ID_i,(x_i,y_i))}$ User A



# MobiShare+: Security Improved System for Location Sharing in Mobile Online Social Networks

With the development of real time localization and mobile computing technology, it becomes increasingly popular for sharing individual locations in mobile online social network (mOSN), which inevitably raises significant concerns on the privacy of users' locations. Recently, Wei et al. provided the MobiShare mechanism to enable flexible location sharing between both trusted social relations and untrusted strangers. Motivated by Wei et al.'s pioneer work, we make a further treatment on privacy-preserving location sharing in mOSN in this paper. We observe that users' real fake identities will be potentially leaked to location service provider in Wei et al.'s work, which may lead to a variety of serious attacks. In order to fix this security issue, we propose a security improved mechanism namely MobiShare+, which employs dummy queries and private set intersection protocol to prevent the OSN service provider and location service provider from learning individual information from each other. Finally, security analysis is provided to clarify that MobiShare+ is secure in terms of location privacy and social network privacy.



relations and locations even if some of the them are dummies. More seriously, if we consider multiple queries without locations updates, the location service provider is able to finally obtain the topological structure of the social network and launch multiple attacks.

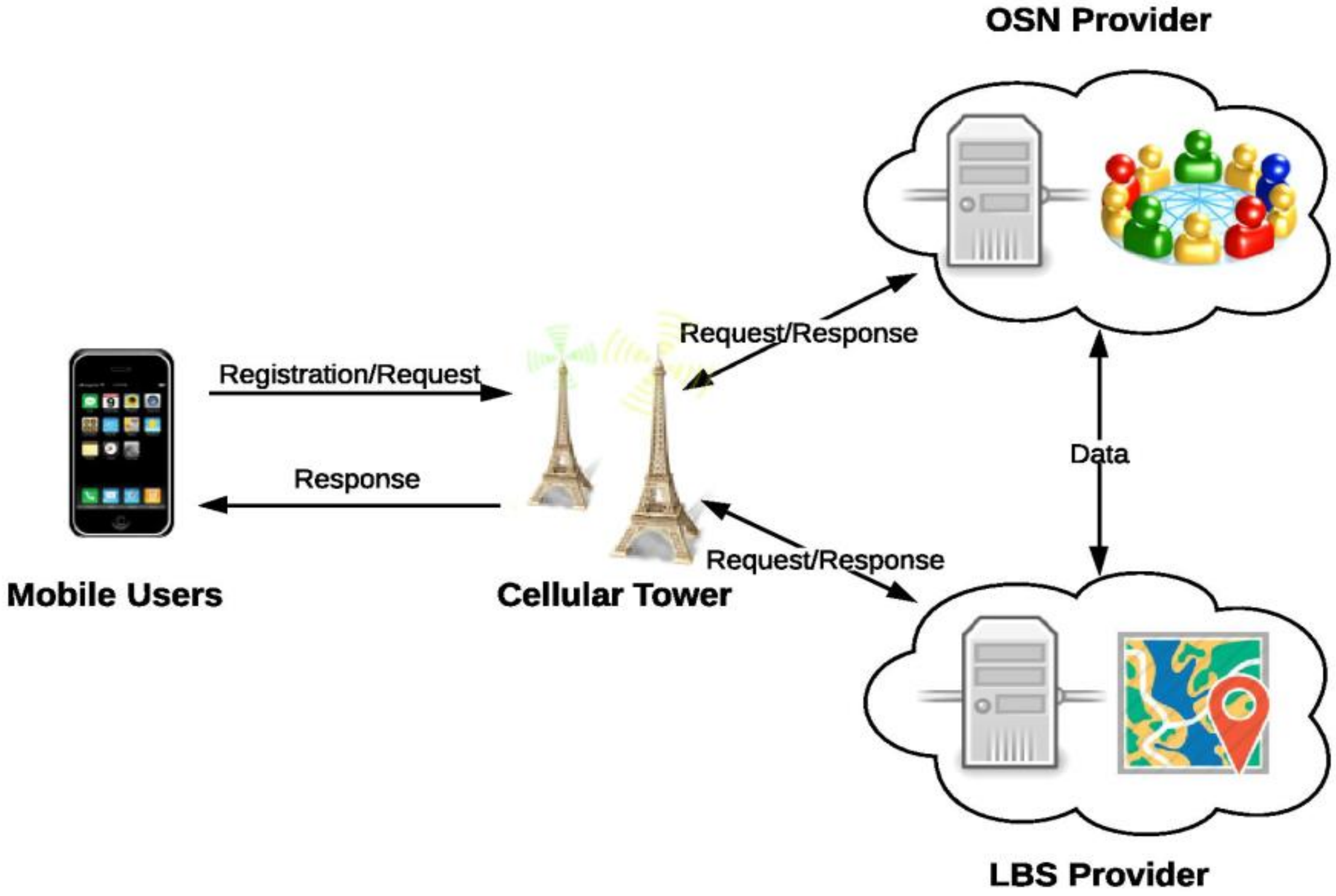


Figure 1: Architecture for Location Sharing in Mobile Online Social Network

# A user sensitive privacy-preserving location sharing system in mobile social networks

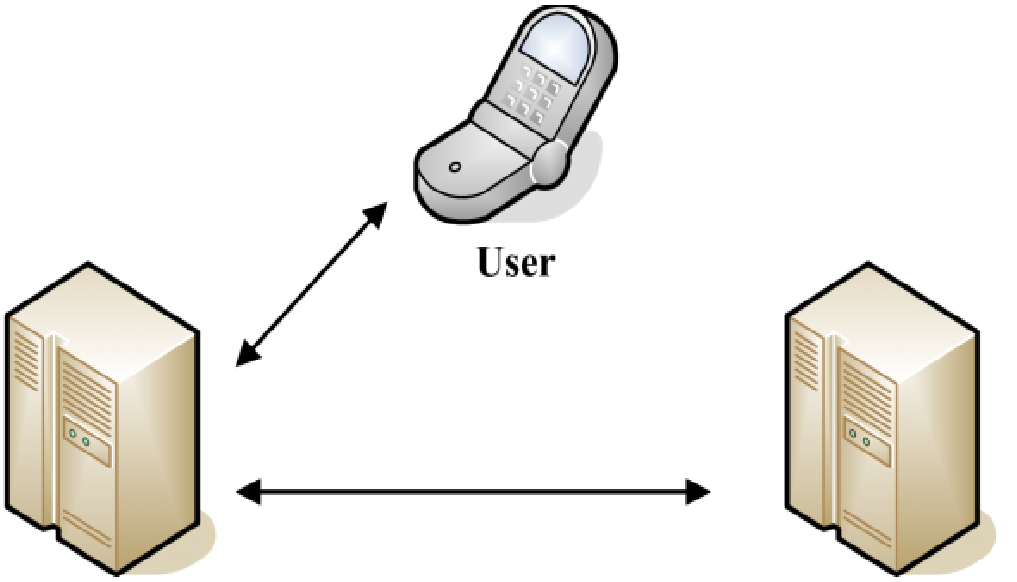
Wei Cherng Cheng[a], Masayoshi Aritsugi[a]*

[a]*Computer Science and Electrical Engineering, Graduate School of Science and Technology, Kumamoto University*
*2-39-1 Kurokami, Chuo-Ku, Kumamoto 860-8555, Japan*

transmission. The proposal considered the cellular tower as a trusted 3rd party server, so it can perform fake users' generation and users' encryption. There are two concerns from the proposal. First, it limits connections with cellular tower only, and other network protocols, such as Wi-Fi, and AP don't suit. Second, a cellular tower doesn't perform as a functional server for specific mobile applications practically. Wernke et al. [12] proposed an arithmetic algorithm

# New Privacy-Preserving Location Sharing System for Mobile Online Social Networks

with malicious users. However, cellular towers are used to establish secure communication with location server for updating user's location, but deployments or upgrades of them are very difficult for the reason that lots of them are distributed in any place and belongs to different telecom operators, which leads to be impractical.



User

**Social Network Server**
**TABLE** userinfo(ID, FID, FKey)
**TABLE** friends(ID, FID)

**Location server**
**TABLE** locationinfo(FID, xy, Sessionkey, $\text{encrypt}_{FKey}(xy)$)

Figure 2. N-Mobishare Architecture

# PLocShare: A privacy-preserving location sharing scheme in mobile social network

Jiazhu Dai
School of Computer Engineering and Science
Shanghai University,
Shanghai, China
daijz@shu.edu.cn

Liang Hua
School of Computer Engineering and Science
Shanghai University,
Shanghai, China
hualiangde@163.com

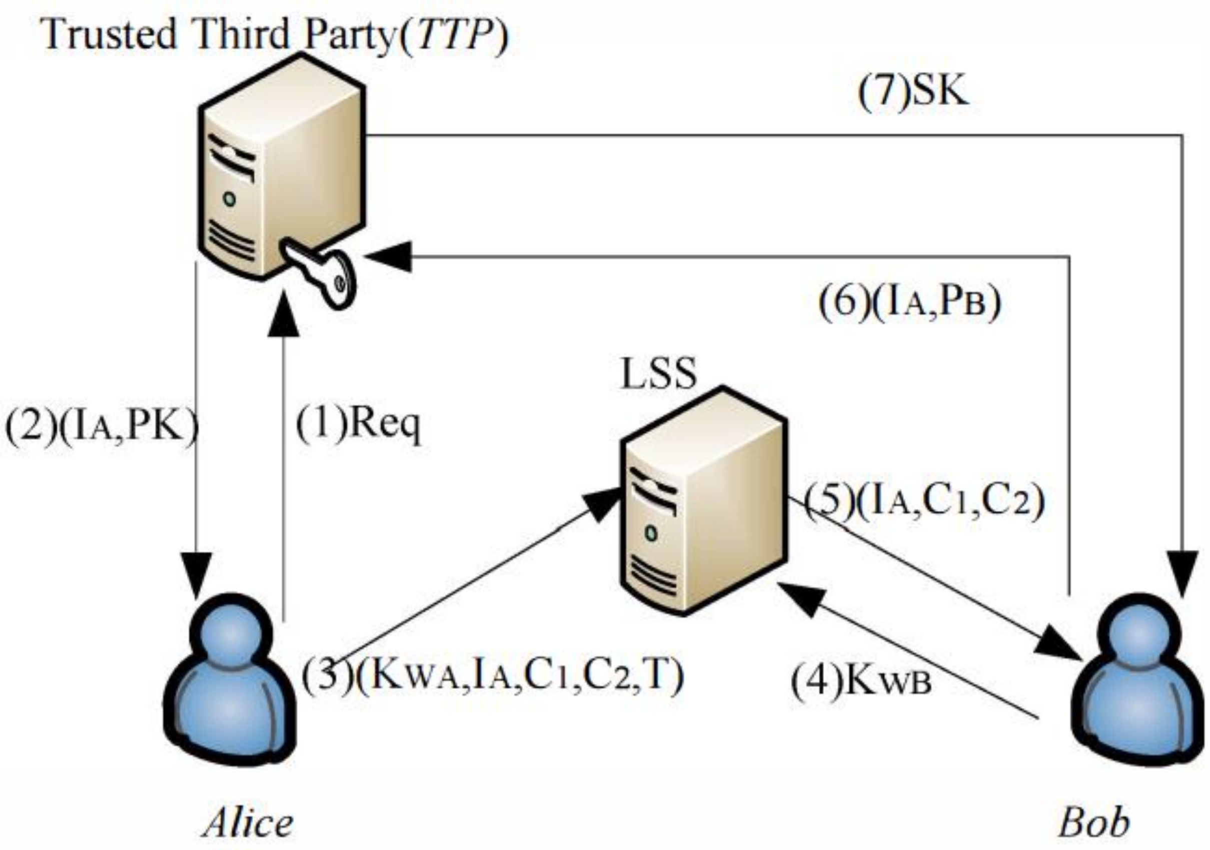
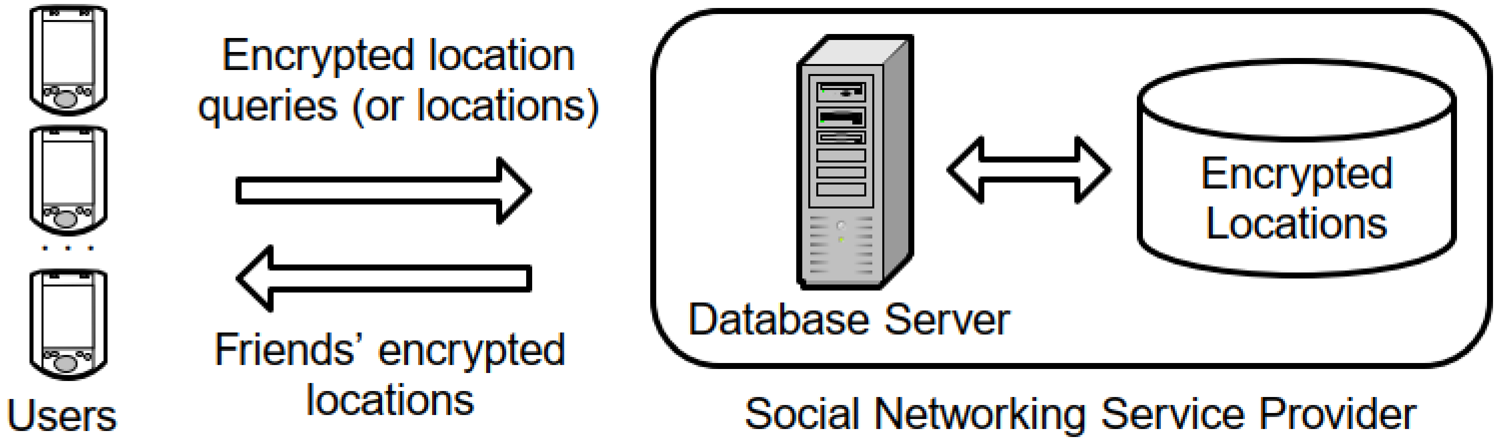


Figure 1. The system model of PLocShare

# Privacy-Preserving Location Sharing Services for Social Networks

Roman Schlegel, *Member, IEEE,* Chi-Yin Chow, *Member, IEEE,* Qiong Huang, *Member, IEEE,* and Duncan S. Wong, *Member, IEEE*


Encrypted location queries (or locations)
Friends' encrypted locations
Users
Database Server
Encrypted Locations
Social Networking Service Provider