

FINE-GRAINED PRIVACY PRESERVING IN MOBILE SOCIAL NETWORKING

Mr.S.M.Londhe¹, Ms.S.C.Chauhan²

¹ Mr.S.M.Londhe, Department of Computer Science & Engineering, EESCOE&T,
Ohar, Aurangabad, Maharashtra, India

² Ms.S.C.Chauhan, Department of Computer Science & Engineering, EESCOE&T,
Ohar, Aurangabad, Maharashtra, India

ABSTRACT

Mobile social networks represent a Cyber-Physical System (CPS), it connects mobile nodes within a local physical proximity by using mobile smart phones as well as wireless communication. In mobile social networks, the mobile users may have face the risk of leaking their personal information and location privacy. Proximity-based mobile social networking mainly refers to the social interaction between mobile users. In this paper we propose new protocol to protect user privacy .here we introduce fairness aware and new protocol blind vector transformation and fine-grained profile matching in which one user match profile with another.

Keyword –fine grained matching, privacy preserving, proximity-based mobile social networking, cyber physical system, mobile social network.

1. INTRODUCTION

Mobile online social networks have gained tremendous momentum in the recent years due to both the wide proliferation of mobile devices such as smartphones and tablets as well as the ubiquitous availability of network services. With the proliferation of mobile devices, mobile social networks (MSNs) are becoming devoted part of our lives. Leveraging networked portable devices such as smart phones and personal digital assistant(PDA) as platforms, MSN not only enables people to use their existing online social networks (OSNs) at anywhere and anytime, but also introduces a myriad of mobility-oriented applications, such as location-based services and augmented reality. Location-aware mobile social networks represent a promising Cyber-Physical System (CPS), which connects mobile nodes within a local physical proximity by using mobile smart phones as well as wireless communication.

To find interesting neighbors and their communications are important functions of social networks. When people join social networks, they first creating his/her profile, then interact with other users. Here each users first find similar interest persons with his/her profile matching. Recently, there are quite a few proposals for *Private Profile Matching*, which allow two users to compare their personal profiles without disclosing his/her private information to each other [6], [5]. In a profile matching scheme, the profile of a user consists of multiple attributes that can be chosen from a public set of attributes (e.g., various interests[5], disease symptoms[7], or friends [8] etc.). However, there are quite a few challenges which make the existing private profile matching solutions less practical in applications. For example, similar to most of the online social network applications, a mobile social networking user is expected to freely search its potential common-interest friends by matching his *interest* with the *personal profiles* of the searching targets rather than making the profile matching directly. As is shown in Fig. 1, Alice has her personal profile, which includes three attributes: age, girl and movie. She is interested in finding a boy with similar age and hobbies. Conversely, Bob also has his own profile and interests. A successful matching could be achieved in case that Alice's profile matches Bob's interest while, at the same time, Bob's profile matches Alice's interest. Such a mapping process could be well supported by the existing online dating social networks, in which a member may seek another member satisfying some particular requirements (e.g., gender, age ranges or even living

location as in [13]). Further, the existing proposals are one-way only and profile matching requires running a protocol twice, with reversed roles in the second run. This two-pass protocol may be exploited by the dishonest user

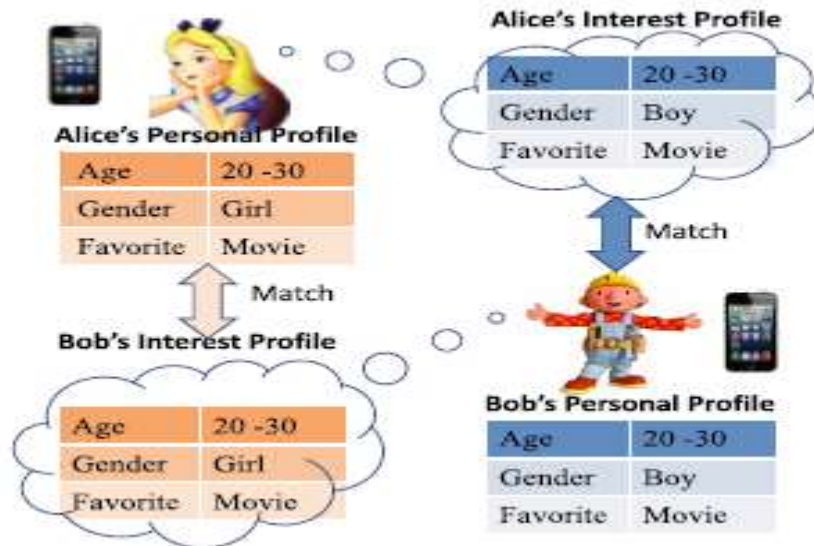


fig 1:friend discovery in mobile social network (msn)

or even a malicious attacker to launch the *runaway attack*, in which a malicious one that wants to learn another user's interests but is unwilling to reveal his own interests can simply abort the protocol in the second round. This runaway attack incurs a serious unfairness issue. The runaway attack may be more challenging in the case of separating user's profile from his interest since matching the users' profile and the interest could only be achieved in two steps.

To solve these challenges and thus further improve the usability of mobile social networks, we present a novel Privacy Preserving and Fairness aware Friend Matching Protocol. In this protocol, a matching process only happens in case that the interests of both of the participants match the profiles of the others. or, no could get any additional information from the protocol unless another Participant is exactly what he is looking for and vice versa. In these schemes, however, cannot distinguish the users with the same attribute(s). For example, there are three users all of watching movie but the no. of movies should be different for each users, to differentiate this use fine grained private matching. In our solution features fine-grained personal profiles in which each attribute/interest is associated with a user specific integer value that indicating the corresponding user's association with this attribute. To provide fine grained profile matching we propose a Max-Distance matching scheme. In which each interest of users have a threshold and find maximum difference between users attribute and compare it with threshold value.

2. SYSTEM, ADVERSARY MODEL:

In this section, we first introduce our system model as well as the adversary model.

2.1 System Model

In mobile social networks, a user launches a query to find the potential friends, when he comes to new places. Before the query, a user should initialize a profile as his inherent characteristic. This profile consists of multiple attributes (e.g., user's occupation, hobbies and other private information), which could be denoted as a vector $P = \{p_1; p_2; \dots; p_n\}$. Here, $p_j (j \in \{1, \dots, n\})$ is an integer, which refers to an attribute of P . When a user issues a query, he firstly generates the corresponding interest vector $I = \{i_1; i_2; \dots; i_n\}$. Note that, similar to a typical search process of online social networks, the user could freely generate different interests for multiple times.

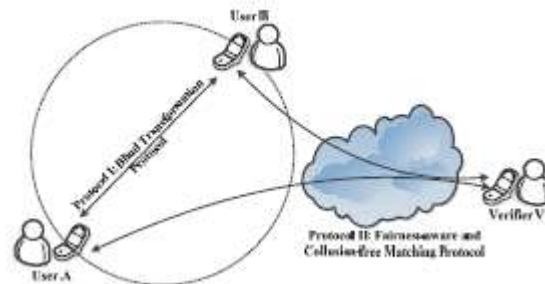


Fig 2.1. System Architecture

In this scheme each user's personal profile consist of multiple attributes that can be chosen from a public set of attributes like various interests , friends , or disease symptoms , these schemes could enable two users to find the intersection or intersection cardinality of their profiles does not providing any additional information to either party. These schemes, however, it cannot well distinguish the each user with the same attribute(s). For example, there are three users all are interested with watching movie (i.e., a common attribute), but they watch two/two/seven per week, respectively. The first two apparently have a better match, but in our friend matching schemes will result in the same level of profile similarity between every two users. We propose *fine-grained* private matching for PMSN to Overcome these challenge. In which each attribute is associated with user specific integer values.

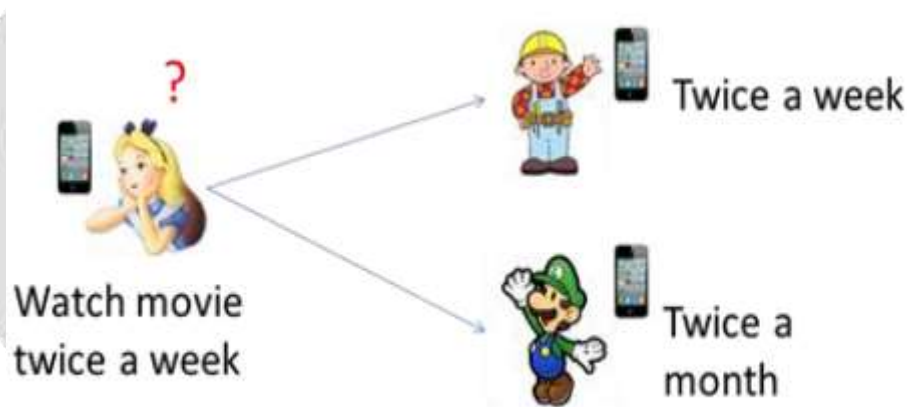


Fig.2.2. Fine grained matching

2.2. Adversary model

The adversary is considered to be curious with others' profile and interest. Therefore, if without an appropriate security countermeasure, the friend discovery process may suffer from a series of privacy threats. In particular, we consider the following adversary model:

1) Privacy Inference from Profile Matching:

The adversary tries to find out the interests or the profiles of the other users during the profile matching process.

2) Privacy Inference from Aborting the Protocol (Run-away Attack):

Under this attack, even with a privacy- preserving profile matching protocol, the adversary aims to infer the private information of another user by stopping the protocol during the friend matching process and performing certain analysis over the information already obtained. This attack will intro-duce a serious unfairness issue since, in a two-pass protocol, the adversary could refuse to send his matching result after obtaining the result from his partner.

3) Collusion Attack:

The adversary may collude with other users to infer the user's private information.

2.3. Paillier cryptosystem

Key Generation The verifier chooses two primes numbers p and q and calculate $N = pq$ and $\lambda = \text{lcm}(p - 1, q - 1)$. It then selects a random $g \in \mathbb{Z}^*N^2$ such that $\text{gcd}(L(g\lambda \bmod N^2), N) = 1$, The entity's Paillier public and private keys are (N, g) and λ , respectively.

Encryption Let $m \in \mathbb{Z}_N$ be a plaintext to be encrypted and $r \in \mathbb{Z}_N$ be a random number. The cipher text is given by $E(m \bmod N, r \bmod N) = g^m r^N \bmod N^2$, (1)

Decryption Given a cipher text $c \in \mathbb{Z}_{N^2}$, the corresponding plaintext can be derived as $D(c) = L(c\lambda \bmod N^2) L(g\lambda \bmod N^2)^{-1} \bmod N$, (2) where $D(\cdot)$ denotes the Paillier decryption operation using private key $sk = \lambda$ hereafter.

3. FINE GRAINED FRIEND MATCHING PROTOCOL

A. Blind transformation algorithm

- Separate users profile and interest profile
- Encrypted each users profile with his/her public key by using paillier cryptosystem
- Vector addition, vector shuffling, and vectorExt done for profile blind ones.
- Compare each user's encrypted profile for matching phase.

B. Max-distance matching protocol

To provide a finer differentiation between within attribute using max-distance matching protocol. Following steps are used for these protocols,

- Set similarity score as zero
- Calculate threshold value for each interest by using $th/2$
- Calculate $\ell_{\max}(u, v) = \max\{|v_1 - u_1|, \dots, |v_d - u_d|\}$
- If $\ell_{\max}(u, v) < \text{threshold}$, then similarity score "1"
- If total score ≥ 3 then "matching"
- Else "not matching"

4. CONCLUSIONS



With increasing popularity of mobile social networks, it is important to develop secure and practical protocols to enable users to effectively interact with each other. In this work, we have developed a novel protocol that will ensure the fairness and the privacy of privacy-preserving interest _ne-grained interest/profile matching in mobile social network. Our future work includes how to provide more security and privacy issues in mobile social networks.

5. REFERENCES

- [1]. L. Kissner and D. Song, "Privacy-preserving set operations," in *Advances in Cryptology_CRYPT0 2005*, pp. 241_257.
- [2]. (2012). *Foursquare* [Online]. Available: <https://foursquare.com/>
- [3]. "gowalla," 2012. [Online]. Available: <http://gowalla.com/>.
- [4]. Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "ESmallTalker: A Distributed Mobile System for System for Social Networking in Physical
- [5]. Proximity," in Proc. of *IEEE ICDCS'10*, Jun. 2010, pp. 468-477.
- [6]. R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare Social network," *Mobile Netw. Appl.*, vol. 16, no. 6, pp. 683_694, 2010.
- [7]. Wei Dong, Vacha Dave, Lili Qiu, and Yin Zhang, "Secure Friend Discovery in Mobile Social Networks." In

- Proc. of *IEEE INFOCOM' 11*, Shanghai, China, April 2011.
- [8]. L. Kissner and D. Song, "Privacy-preserving set operations," in *Advances in Cryptology_CRYPTO 2005*, pp. 241_257.
- [9]. D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Reading, MA, USA: Addison-Wesley, 1997. (2012). *Perfect-Match* [Online]. Available: <http://www.perfectmatch.com>.
- [11]. N. Eagle and A. Pentland, "Social serendipity: Mobilizing social soft- ware," *IEEE Pervas. Comput.*, vol. 4, no. 2, pp. 28_34, Apr. 2005.

BIOGRAPHIES

	<p>Mr.S.M.Londhe received his BE in Information Technology from University of Pune, India and pursuing ME(CSE)- from EESCOE&T ,BAMU,Aurangabad, India ,He is currently working as Lecturer at Matoshri Aasarabai Polytechnic,Nashik</p>
	<p>Ms.S.C.Chauhan pursuing ME(CSE) from EESCOE&T ,BAMU,Aurangabad, India ,He is currently working as Lecturer at Government Polytechnic,Jalana.</p>