Fine Grained Privacy Preserving with Friend Matching Protocol in mobile social networks

Fayisa M K, Femitha mol A M

***Abstract*— Mobile social networks represent a Cyber-Physical System (CPS), it connects mobile users within a local physical proximity by using mobile phones. Proximity-based mobile social networking (PMSN) mainly refers to the social interaction between physically proximate mobile users. In mobile social networks mobile nodes are connected by smart phones as well as wireless communication. However in this networks mobile nodes may face a big problem like leaking of their privacy information's and location privacy. In this paper we propose new protocol to protect users privacy within an efficient way. Here we introduce new protocol Blind vector transformation which could hide correlation between original and transformed result and fairness aware interest and profile matching in which allow one party to match profile with another. And also provide how to provide fine grained profile matching.**

***Index Terms*— Proximity-based mobile social networking, profile matching, privacy, fine grained matching, secure communication.**

I. Introduction

In the last decade, the number of users of online social networking sites and of mobile phone services has increase rapidly. 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. Among them, an important service is to make new social connections/friends within physical proximity based on the matching of personal profiles. For example, MagnetU is a MSN application that matches one with nearby people for dating or friend-making based on common interests. In such an application, a user only needs to input some (query) attributes in her profile, and the system would automatically find the persons around with similar profiles. The scopes of these applications are very broad, since people can input anything as they want, such as hobbies, phone contacts and places they have been to. The latter can even be used to find “lost connections” and “familiar strangers”.

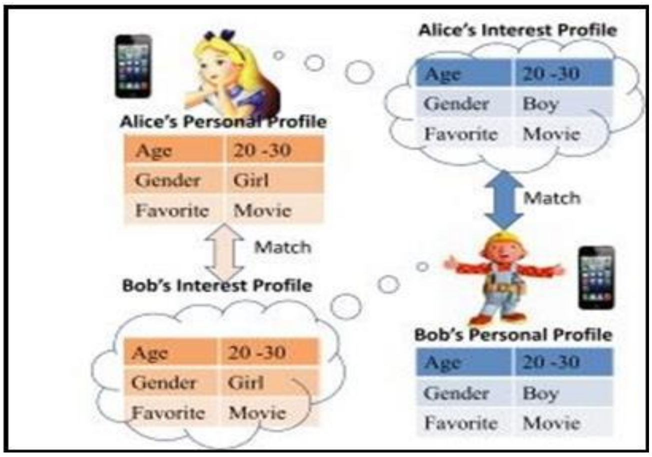

Fig. 1. Friend Discovery in Mobile Social Networks

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 a few challenges which make the existing personal profile matching solutions less applicable practically. For example, similar to most of the online social network applications, in a mobile social networking user is freely seeking its potential Common-interest friends by matching his/her *interest* with the *personal profiles* of the searching users rather than making the profile matching directly. As is shown in Fig. 1, Alice has her own personal profile, which contains three attributes: age, girl and movie. She is seeking 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 interest 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 dating social networks. Further, these existing proposals are one-way only and profile matching requires running a protocol twice, with reversed in the second run. This two-pass protocol may be produce by the dishonest user or malicious user to launch the *runaway attack*, in which a malicious one that wants to learn another user's interests but he/she does not reveal his/her own interests can simply stop the protocol in the second run. This runaway attack causes serious unfairness issue.

To solve the 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

Manuscript received September 05, 2014.
Fayisa M K, Computer Science, ICET,Mulavoor, Ernakulam,India
Femitha mol A M, Asst.Professor IT, ICET,Mulavoor, Ernakulam,India

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.

II. SYSTEM MODEL AND PRELIMINERIES

In this section we introduce our system model as well as the important aim of our work. Before explain our protocol first introduce a paillier cryptosystem. Here paillier encryption and decryption are used to generate public key and private key of each users.

A. *System model*

In mobile social networks, a user produce a query to find the potential friends in the physically proximate networks, when he/she comes to a new places. Before the query, a user must introduce a profile as his/her inherent characteristic. This profile consists of multiple attributes (e.g., user's occupation, symptoms hobbies and other private information), which could be denoted as a vector P = $\{p1, p2, \ldots, pn\}$. Here, $pj(j = 1, \ldots, n)$ is an integer, which refers to an attribute of P. When a user introduce a query, he firstly generates the corresponding interest vector I = $\{i1, i2, \ldots, in\}$.

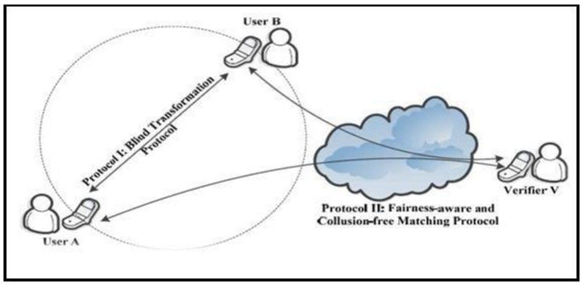
User B
Protocol I: Blind Transformation Protocol
Verifier V
Protocol II: Fairness-aware and Collusion-free Matching Protocol
User A

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 [2], friends [3], or disease symptoms [4], 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 users 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 [2]–[4] 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.

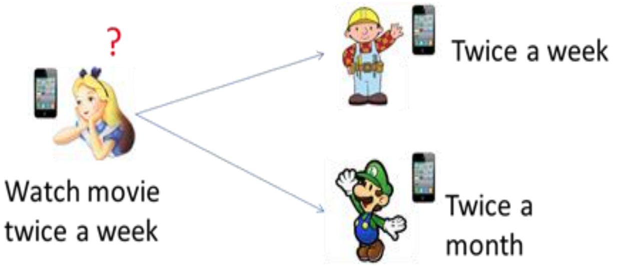

Fig 2.2 fine grained matching

B. *Paillier cryptosystem*

Key Generation. The verifier chooses two primes numbers p and q and calculate $N = pq$ and $\lambda = \mathrm{lcm}(p - 1, q - 1)$. It then selects a random $g \in Z{*}N2$ such that $\gcd(L(g\lambda \bmod N2), N) = 1$, The entity's Paillier public and private keys are _N, g_ and λ, respectively.
Encryption. Let $m \in ZN$ be a plaintext to be encrypted and $r \in ZN$ be a random number. The cipher text is given by $E(m \bmod N, r \bmod N) = gmrN \bmod N2$, (1)
Decryption. Given a cipher text $c \in ZN2$, the corresponding plaintext can be derived as $D(c) = L(c\lambda \bmod N2)\, L(g\lambda \bmod N2) \bmod N$, (2) where $D(\cdot)$ denotes the Paillier decryption operation using private key sk = λ hereafter.

III. 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 users 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 protocol,

- Set similarity score as zero
- Calculate threshold value for each interest by using th/2
- Calculate $\ell\max(u, v) = \max\{|v1 - u1|, \ldots, |vd - ud|\}$
- If $\ell\max(u, v) <$ threshold, then similarity score "1"
- If total score>=3 then "matching"

- Else “not matching”

IV. RELATED WORKS

Dong et al. proposed to match two PMSN users based on the distance between their social coordinates in an online social network [6]. these scheme matching is based on computing the similarity between two users coordianates.These scheme needs a trusted authority to provide coordinates. In these scheme protocol ensures that the initiator can only learn the comparison result between the estimated proximity and the threshold

In [5], Li et al. proposed FindU, a privacy-preserving personal profile matching in mobile social networks. Here by using secure multi-party computation (SMC) techniques, it can achieves that, an initiating user can find from a group of users the one whose profile best matches with his/her interest profile. Here we introduce an initiator and some coordinators and initiator checks the matching profile of each coordinators.

In [3] and it proposed the concept of privacy preserving in a distributed way, We *do not assume the existence of a trusted third party* during the protocol run; In existing systems usually all the users directly publish their complete profiles for others to search. Propose new method called FindU all parties carry out profile matching in a completely distributed way. They may cooperate with each other In these existing works, we separate users’ profiles from their interest for the first time. Further, we propose a blind vector transformation and maximum distance matching protocol to provide a better security for personal profiles.

V. CONCLUSION

A mathematical programming model is used to improve the navigation effectiveness of a website while minimizing changes to its current structure. Transformation and personalization approaches are integrate in this paper. So changes can acquire all users who can use the website. To provide significant improvements to user navigation by adding new links and also repairing the existing links. The main goal achieved is that complete website reorganization couldn’t radically change the location of familiar items.

REFERENCES

[1] “foursquare,” 2012. [Online]. Available: https://foursquare.com/.

[2] “gowalla,” 2012. [Online]. Available: http://gowalla.com/.

[3] Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, “ESmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity,” in Proc. of *IEEE ICDCS’10*, Jun. 2010, pp. 468-477.

[4] R. Shokri, G. Theodorakopoulos, C. Troncoso, J. P. Hubaux, and J.- Y. Le Boudec. Protecting location privacy: Optimal strategy against localization attacks. in Proc. of *ACM CCS’12*, pp.617-627, 2012.

[5] M. Li, N. Cao, S. Yu, and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” in Proc. Of *IEEE INFOCOM’11*, Shanghai, China, April 2011.

[6] 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.