Privacy Preserving Friend Matching Protocol in Social Networks

Saranya S [1], Manojkumar M [2], Saravanakumar M [3]
1Assistant Professor, [2][3] UG Scholar, Department of C.S.E SNS College of Engineering, Coimbatore.

Abstract- Social networks connect nodes within a local physical proximity by using wireless communication. It sophisticates the user face to face social interactions. Users may face the risk of leaking their personal information and their location privacy. In existing system novel blind vector protocol, which blindly compare the user profile without ensure the information leakage. By introducing Fine-Grain protocol, information leakage will be protected by private interaction. Based on it, we propose our privacy-preserving and interest friend matching protocol, which allows one party to match its interest with the profile of another, without revealing its real interest and profile.

Index Terms—Privacy Preserving, Friend Discovery, Mobile Social Networks

I INTRODUCTION

Social network grows tremendous among the environment nowadays in both computer and mobile devices available in Network Service. In social network, nodes within physical proximity where connected using wireless communication. Users may share the locations in real time using wireless localization techniques. Location aware social network represents promising Cyber-Physical System (CPS), which allow user to experience face to face social interaction. Profile matching is more than important for fostering the wide use of social networks because finding the nearby individuals of the similar interests is always the first step for any social networking.

The existing social network systems pay little heed to the security and privacy concerns associated with revealing one’s personal social networking preferences and friendship information to the ubiquitous computing environment. In particular, in mobile social networks, the mobile users may face the risk of leaking of their personal information and their location privacy. Under this circumstance, the attackers can directly associate the personal profiles with real persons nearby and then launch more advanced attacks. Existing researches show that loss of privacy can expose users to unwanted advertisement and spams/scams, cause social

reputation or economic damage, and make them victims of blackmail or even physical violence.

Recently, there are quite a few proposals for Friend-Interest Matching, which allow two users to compare their personal profiles without revealing private information to each other. In a typical private profile matching scheme, the personal profile of a user consists of multiple attributes chosen from a public set of attributes. The private profile matching problem could then be converted into Private Set Intersection (PSI) or Private Set Intersection Cardinality. In particular, two mobile users, each of whom holds a private data set respectively, could jointly compute the intersection or the intersection cardinality of the two sets without leaking any additional information to either side. 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.

Fig. 1. Alice has her personal profile, which includes three attributes: age, girl and movie. She is interested in

Gender Boy
Favorite Movie
Age 20-30
Favorite Movie
Gender Boy
Age 20-30
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. 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 or even a malicious attacker to launch the runaway attack, in which a malicious one that wants to learn another user’s interests is simply out 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 the above mentioned challenges and thus further enhance the usability of mobile social networks, [2] we present a Fine Grained Privacy Preserving and Fairness-aware Friend Matching Protocol. In the designed protocol, a successful matching only happens in case that the interests of both of the participants could match the profiles of the others. In other words, no one can learn any extra information from the protocol unless another participant is exactly what he is looking for and vice versa. Our work is motivated from a simple observation that if two vectors match, they will still match no matter whether they are transformed in the same way (e.g., add or remove a randomly generated vector) or shuffled with the same order.

2. PROPOSED PRIVACY-PRESERVING AND FRIEND INTEREST MATCHING PROTOCOL:

In this section, we introduce about the protocols:

2.1 PROTOCOL OVERVIEW:

The proposed protocol comprised of two different protocols, includes Protocol I: Friend-Interest matching protocol; Protocol II: Blind Vector Transformation Protocol. The basic idea of the Friend – Interest Matching Protocol which allows two different user to compare their profiles based on their common interest without reveal their personal interest by following the series of privacy.

E.g. Adding Random vector by their interest and expectations.

The major challenge of this profile comparison is collision attack and privacy risk. Also how blind vector will hide the personal information.

2.2 SYSTEM INITIALIZATION PHASE:

In system initializing phase, third party will generate private and public key sets denoted as (a0,b0) and (a1,a0) respectively.

2.3 PROPOSED FRIEND-INTEREST MATCHING PROTOCOL

In this protocol, two different profiles v1 and v2 has their own interest and privacy features. A third party will handle the key features to manage the privacy of the profiles. Using fine-grain protocol, each profile consist of their own information and interest. Since in existing system, profiles will be matched randomly. But in this protocol, profile-matching achieved through based on interest and their matching expectations. Multiple vectors v(n1,n2………Nm) will be compared at the same time for the better result.

Security measures are very well improved in the proposed systems. Private-set interaction has keep the profile information hidden.

- Profile information default as private for the unknown profiles.
- Collision attack will be carried through.

2.4 BLIND TRANSFORMATION PROTOCOL

In the blind transformation phase, each participant will encrypt his profile by using his public key and provide it to his partner for blind transformation. In the follows, [1] we introduce the blind transformation process by taking U0 transforming U1’s profile and his own interest as an example. It is similar for U1 to blind transform U0’s profile. Ua performs Encrypt (Pa, Pb) to encrypt his profile Pab, which is denoted as Pab. Ua sends Pb and Pab to Ub. Then, Ub performs the following blind transformation operations:

- Blind Add: U0 generates a random vector r0, and then performs Encrypt(r0,Pa). After VecAdd(b0,r0) by adding f r0b and r0 to Pa and eb0, that, U0 calculates Pa = VecAdd(Pa,r0b) respectively.
- Blind Append: U0 generates a random vector yb of length l0, where l0 is a predetermined security parameter, then performs yb = Encrypt(yb,Pa) to get VecExt .
• Blind Reverse: $U_b$ randomly selects $k_b \in \{1,2,\ldots, l\}$ and performs $\text{Vec}_{\text{Rev}}(y_b, k_b)$, then obtains $P_b = \text{Vec}_{\text{Rev}}(I_b, y_b)$.
• Blind Shuffle: $U_b$ performs $I'_{\text{sh}} = \text{Vec}_{\text{Shuffle}}$ and $P'_{\text{a}} = \text{Vec}_{\text{Shuffle}}(P_a)$ with the same order.

After performing this process, $U_b$ finishes the blind transformation of $P_a$ and $I_b$. In the same time, $U_b$ also encrypts his profile and $U_b$ follows the same strategy to make a blind transformation towards $P_b$ and $I_b$.

Note that, among the above four operations, $\text{Vec}_{\text{Add}}$ and $\text{Vec}_{\text{Shuffle}}$ are used to conceal the original value of $P_a$ and prevent $U_b$ from obtaining the transformation ways of $P_a$ and $P'_{\text{a}}$. $U_a$ (or $U_b$) can still obtain the correct number of matched interests and profiles since $P_a$ and $I_a$ (or $P_b$ and $I_b$) follow the same transformation pattern.

However, if only with $\text{Vec}_{\text{Add}}$ and $\text{Vec}_{\text{Shuffle}}$, an dishonest participant could still infer another party’s profile information without revealing his own profile information by stopping the protocol as long as he receives the matching information between his interest and another party’s profile, which is called as runaway attack. Runaway attack will lead to serious unfairness issues. To achieve fairness of the proposed protocol, we further introduce $\text{Vec}_{\text{Ext}}$ and $\text{Vec}_{\text{Rev}}$, which are used to hide the exact interest/profile matching numbers. In particular, on $U_a$'s side, $\text{Vec}_{\text{Ext}}$ introduces extra $l_b$ ones to the original matching result while $\text{Vec}_{\text{Rev}}$ introduces $k_b$ mismatching. Therefore, the actual matching result is updated to $s = s + l_b - k_b$ for $U_a$, and $s = s + l_b - k_a$ for $U_a$. The blind transformation phase is summarized in Algorithm 1.

The proposed blind transformation phase by using a simple example, in which $U_a$’s profile $P_a$ and $U_b$’s interest $I_b$ are compared. To prevent the privacy leaking of $P_a$ and $I_b$, $P_a$ and $I_b$ are encrypted firstly and then are added with a randomly generated vector $r_a$. Since both of $P_a$ and $I_b$ are encrypted with Paillier cryptosystem, the homomorphic property guarantees that the comparison result will not be changed after adding the same $r_a$. After that, $P_a$ and $I_b$ are shuffled and shuffled by following the same way. It is obvious that, such a transformation will not change the matching results.

### III EVALUATION

We implemented our protocol in Java for portability and evaluated it on a laptop with Intel Core i3-330m (2.1GHz) and 2GB RAM. The Paillier encryption library was based upon [10]. We modified it and used the fast variant of Fiat- Schoenfeld's execution time on fair matching phase for different number of attributes (ms) is shown in Fig. 3.1.

![Graph showing execution time on blind transformation for different number of attributes (ms)](image)

### IV CONCLUSION

In this work we have included how to provide fine-grained, Friend-interest/profile matching protocols and privacy issues and also collision and Run-Away attack can overcome in socialnetwork.

### REFERENCES