# Privacy Preserving Friend Matching Protocol in Social Networks

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

***Abstract*- Social networks connects 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.

[1]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.

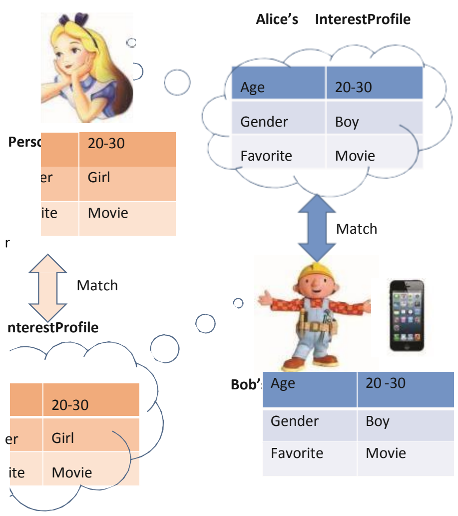



Fig. 1, Alice has her personal profile, which includes three attributes: age, girl and movie. She is interested in finding a boy with similar age and hobbies. Conversely, Bob also has his own profile and interests. A successful matching could be achieved in case that Alice's profile matches Bob's interest 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 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 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 $(a_{k0},b_{k0})$ and $(a_{k1},a_{k1})$ 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 $U_b$ transforming $U_a$'s profile and his own interest as an example. It is similar for $U_a$ to blind transform $U_b$ 's profile. Ua performs Encrypt (Pa, $p_{ka}$) to encrypt his profile $P_a$, which is denoted as $P_{'a}$. $U_a$ sends $P_{'a}$ and $p_{ka}$ to $U_b$. Then, $U_b$ performs the following blind transformation operations:

- Blind Add: $U_b$ generates a random vector $r_b$, and then performs Encrypt($r_b$,$p_{ka}$). After $Vec_{Add}(I_b,r_b)$ by adding f rb′ and $r_b$ to P′a and $e_{Ib}$, that, $U_b$ calculates $Pa = Vec_{Add}(P'_a,r_b')$ respectively.
- Blind Append: $U_b$ generates a random vector yb of length $l_b$, where $l_b$ is a predetermined security parameter, then performs $y_b' =$ Encrypt $(y_b,p_{ka})$ to get $Vec_{Ext}$ .

- Blind Reverse: $U_b$ randomly selects kb ∈ {1,2,•••, l2} and performs $Vec_{Rev}(y_b,k_b)$, then obtains $I'b= Vec_{Ext}(I_b,y_b)$.
- Blind Shuffle: $U_b$ performs $I''_{eb}= Vec_{Shuffle}$ and$P''a=Vec_{Shuffle}(Pf_a)$ with the same order.

After performing this process, $U_b$ finishes theblindtransformation of $P_a$ and $I_b$. In the same time, $U_b$alsoencryptshisprofileand$U_a$followsthesamestrategyto make a blind transformation towards $P_b$ and$I_a$.

Note that, among the above four operations, $Vec_{Add}$and$Vec_{Shuffle}$ are used to conceal the original value of Paandprevent $U_b$ from obtaining the transformation ways of$U_a$by linking Pa and P″1. $U_a$ (or $U_b$) can still obtainthecorrect number of matched interests and profiles since $P_a$ and $I_b$(or $P_b$ and $I_a$) follow the same transformation pattern.

However, if only with $Vec_{Add}$ and $Vec_{Shuffle}$, adishonestparticipant could still infer another party'sprofileinformation without reveal his own profile informationbystopping the protocol as long as he receives thematchinginformation between his interest and anotherparty'sprofile, which is called as runaway attack. Runaway attackwillleadtoseriousunfairnessissue.Toachieve fairness of the proposed protocol, we furtherintroduce$Vec_{Ext}$ and $Vec_{Rev}$, which are used to hide theexactinterest/profile matching numbers. In particular, on$U_a$side, $Vec_{Ext}$ introduces extra lb ones to originalmatchingresult while $Vec_{Rev}$ introduces kb mismatching.Therefore,the actual matching result is updated to $s_b= e_b+ l_b - k_b$ for $U_b$ and$s_a=e_a+l_a - k_a$ for$U_a$.Theblindtransformation phase is summarized in Algorithm1.

The proposed blind transformation phase by usingasimple example, in which $U_a$'s profile Pa and $U_b$'sinterest$I_b$ 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 witha randomly generated vector $r_a$. Since both of $P_a$ and $I_b$areencrypted with Paillier cryptosystem, thehomomorphicproperty guarantees that the comparison result will notbechanged after adding the same $r_a$. After that, $P_a$ and $I_b$areextended and shuffled by following the same way. Itisobvious that, such a transformation will not changethematchingresults.

## III EVALUTION

We implemented our protocol in Java for portabilityandevaluated it on a laptop with Intel Core i3-

Paillier scheme as proposed in [10]. We evaluatedtherunning time of our protocol in NovelBlindTransformation, Friend Interest Matching andBlindLinear Trans- formation phase. The algorithm usedinBlind Shuffle is Knuth Shuffle. We use it in ordertoguarantee the randomness inpermutation.

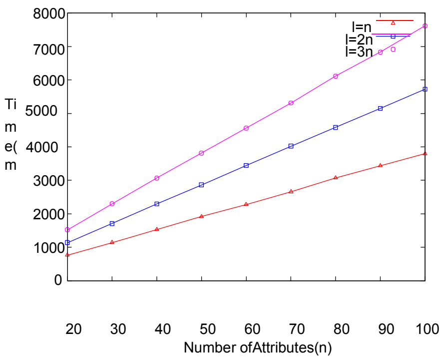
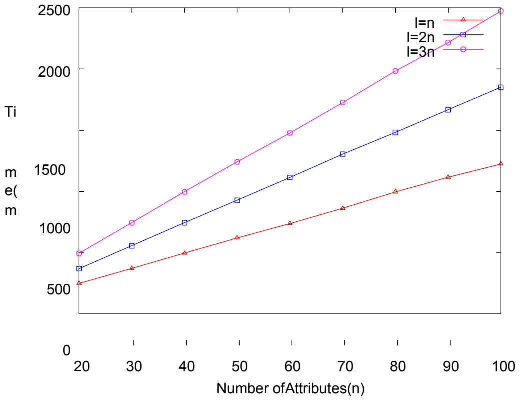



Fig: 3.1 Execution Time on Blind TransformationforDifferent Number of Attributes(ms)




330m(2.1GHz)and 2GB RAM. The Paillier encryption library wasbasedupon[10].WemodifieditandusedthefastvariantofFig:3.2 Execution Time on Fair Matching phaseforDifferent Number of Attributes(ms)

## IV CONCLUSION

In this work we have includes how to providefine-grained, Friend -interest/profile matching protocolandprivacy issues and also collision and Run-Awayattackcan overcome in socialnetwork.

## REFERENCES

[1] Haojin Zhu and Suguo Du, Muyuan Li "Fairness- aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Network," in IEEE TETC, VOL:1 NO:1,Dec 2013.

[2] 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.