Secure and Privacy-Preserving Matchmaking protocol for Mobile Social Networks

JohnBosco Aristotle Kanpogninge Ansuura[a], Xia Qi[b]
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, 611731, China
ajansuura@gmail.com, bxiaqi@uestc.edu.cn

Richmond Martei Tei-Ahontu
School of International Business
Southwest University of Finance & Economics
Chengdu, China
rmta@admin24.com

Benjamin Klugah-Brown
School of Computer Science and Engineering
University of Electronic Science and Technology of China
Chengdu, 611731, China
bklugah@gmail.com

Abstract—Mobile social networking has changed the way people communicate in recent years. Matchmaking service innovates people communication mode in terms of colleague networking, making new friends and many other scenarios. Although this new paradigm brings enormous benefits for enterprises and individuals, how to preserve the user's privacy becomes a key challenge for all parties involved. Most important, user's sensitive information should not and cannot be leaked to any other untrusted party or users cannot take advantage of the system to learn sensitive information.

Keywords-privacy-preserving; matchmaking; security, mobile social networks; hybrid architecture

I. INTRODUCTION

Data privacy protection has always been an issue in the area of information security. Privacy is also legally considered as a fundamental human right [1]. In this scenario privacy is highly essential. Mobile social networking is social networking where individuals with similar interests chat and connect with one another through their mobile phone, tablet and many more smart devices. Previous and most current Mobile Social Network give less attention to security and privacy issues linked with exposing users personal social network attributes and information to the Global community of computing. Matchmaking is a major constituent in mobile social network. This is because locating a user nearby with similar interest is considered as the first phase in mobile social networking. According to [2], the mobile user may face the risk of leaking their personal information and their location privacy information. Under this circumstance, the attackers can directly associate the personal profiles with real persons nearby and launch more advanced attacks. In recent times, there has been several research attempts [2-16] in proposing protocols to preserve privacy during a matchmaking when users compare their personal attributes or likes without disclosing their private information to one another.

In mobile social networks, matchmaking a personal attribute may consist of various interest of users like movies, books, food and places they like visiting and many more. However, there are some challenges with existing protocols which requires long computational time before a secure match is established.

It is in this direction that the author presents the idea of a Secured and Privacy Preserving Security protocol in Mobile Social Networking for Matchmaking. In designing the protocol, a successful matching will be considered to take place only when both interests of the users match the profiles of one another.

The protocol for matchmaking in mobile social network will be based on the following two cardinal points.

1. Designing a protocol suitable for resource constrained mobile social network.
2. A protocol having less communication as well as ensuring privacy by making user reveal no unnecessary private information to other users in order to find new friends. A number of test will be performed on the protocol and validated its effectiveness, efficiency in mobile social network and in the area of information security.

The rest of the paper is organized as follows. Section II presents the problem statement in the form of models and design goals. The design is described in section III. Section IV presents the security analysis and performance evaluation. Section V is the conclusion of the work.

II. RELATED WORK

The matching of attributes in MSN can be address using three main architectures. The simplest is to using a trusted central server which is involved in every step of the matchmaking process, by collecting attributes, performs matchmaking and informing the users of a match. In the second approach, the distributed architecture, the users determine the attributes on their mobile devices which perform the match and notifies their owners of a match. The hybrid architecture employs a Trusted Server only for the purpose of management. Thus, the trusted server certifies users and revokes cheating clients. Social Serendipity [3], this protocol deploys a trusted server which contains users' profiles and user defined matchmaking preference. The server computes the similarity of nearby users' profile and notify users in close proximity with similarities in profiles exceeding a threshold. The server is involved in every step of the matchmaking process thereby detecting which two users are in close proximity and having a common interest making this a limitation of this system.

In 2009, MobiClique [4] proposed an improved system to overcome the limitations of [3]. In their system a middleware is included to allow mobile phone users to connect to other over ad-hoc networks to exchange social network identity information and forward messages. The innovation in [4] is such that the server is away from the matchmaking process. Setting up this scenario is such that, a server, e.g. Facebook, which assigns identifiers to the users allows users to store their profile information on their smart devices and perform profile exchange with the nearby user using Bluetooth or WIFI. A friendship is created based on the user profiles acquired.

However, this application does not put into consideration an adversary attack. It assumes that all users are trusted, and ignores privacy and security. This means that anyone in range can intercept the information and perform a mischievous attack with it. The protocol is going to address this challenge which will make sure that others do not get to know of any information if their interest do not meet the requirement of the other users.

Furthermore, [5] identified three main approaches namely oblivious polynomial evaluation, oblivious Pseudo Random functions and Commutative Encryption.

In oblivious polynomial Evaluation that is reiterated by [6] that is dated back to the FNP scheme where a client and a server computes their intersection set such that the client and server learns nothing. In this case additive homomorphic encryption is used to obliviously evaluate a polynomial that represent clients input.

Subsequently Kissner et al [7] proposed a scheme that involves set intersection, cardinality and over-threshold operations which is later improved by Sang et al in [8].

Ye et al [9] extended the FNP scheme to a distributed private matching scheme which is followed up by [10] focused on reducing the complexity in the malicious model. However, none of these schemes achieved linear computational complexity in terms of encryption operations whiles relying on homomorphic encryption.

Furthermore, Li et al in [11] proposed an unconditionally secure multi-party PSI scheme. Their idea is similar to the one proposed by [7] where the inputs are shared among all parties using secret sharing and computations done on these shares.

Subsequently, Narayanan et al in [12] improved the work by [11] presenting a scheme using the same idea of FNP and also proposed an N-party PCSI scheme. Later, Shaneck et al in [13] proposed using secret sharing to compute dot product securely, but assume that trusted third parties exist. Their scheme however had low computational complexities with high communication cost.

The second approach, oblivious Pseudo Random functions, is adopted by Hazay et al in [14]. Their work looked at a situation where two parties securely computes a pseudo random function where one of them holds the key whiles the other provide the inputs, which is the set of elements. They are able to achieved linear complexity with respect to the set size, but the number of exponentiations are large. Jarecki et al in [15] proposed a scheme with a sufficiently large set size and having achieved a complexity smaller than FNP hence improving its efficiency.

Later, Cristofaro et al [16] proposed a construction using PSI based on blind RSA signatures. The server computes for the client's inputs and a one-time RSA signing Key of the server. Their scheme is more efficient than previous works but couldn't achieve PCSI.

Commutative Encryption being the final approach is adopted by Agrawal et al [17] to realize PSI and PCSI in information sharing between two databases. A commutative encryption scheme has the following property: and used a keyed one-way hash function to generate a mapping for each element such that no one knows the key.

Later, Vaidya et al in [18], extended their scheme to N-party setting. Arb et al in [19] applied the idea to detect friend of friends in Mobile Social Network by using deterministic approach thereby has low security compared to the commutative encryptions.

III. PROBLEM STATEMENT

A. System model

The system architecture consists of Users (U), mobile devices, identity signer (IDS) and private interest Signer (PIS) as shown in figure 1.

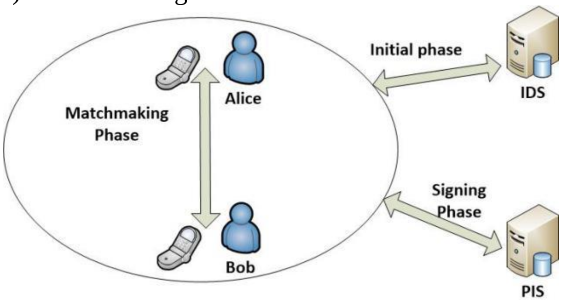

Figure 1. system architecture

- *Users (U):* is a set of registered users, and each user is equipped with a mobile device. Some users may be malicious trying to infer other information on the system by utilizing the vulnerabilities. There are also semi-honest users trying to learn others' private attributes from the messages sent to them. The users determine attributes and compute the RSA signature.
- *Mobile Devices:* Each device has its owner's attributes set configured prior to the matchmaking. The security of these devices are sole the responsibility of the owners.
- *Identity Signer (IDS):* This is a trusted third party (TTP) which assigns an identifier and a certificate to identify each user. Users sends their personal information including their username and generated RSA public key to the IDS who assigns pseudo-id , where is the user index that is is Bob's ID and

certificate to each user. This TTP learns about identity (ID) information only. This helps to identify and authenticate a user eliminating possible impersonation and non-repudiation claims by users.

- *Personal Interest Singer (PIS):* This is responsible for signing users' interest, and will help authenticate that the user's interest has been certified and it is not emanating from an arbitrary interest. These are kept in the PIS database. The PIS provides a web page for users to create and/or look up the names of their interests. Before a user asks the PIS to sign their matchmaking information, they first looks up the web page to see if their interests already exist and for interest standardization purposes. For the interests that already exist, they just re-use the existing ones. For the non-existing interests, they creates their own interest names on the page, and the PIS assigns an ID for each interest. A user submits his/her valid identifier, which he/she gets from the ID signer, and the names of their interests, which they get from the web page, to the PIS. The PIS creates corresponding interest IDs and signatures and then sends them back to the user. If a user frequently changes his/her interests, it is most likely that he/she does not use his/her real information, and he/she just wants to exploit other people's interests [4] which is managed by the PIS.

B. The Game for Attribute Detection

Here denote the set of users who own the targeted attribute a. A picks a target user ∈ and wants to find out the attribute by communicating with Now , define the

Attribute Detection Game for a randomized, polynomial-time adversary A as follows:

Step 1: The adversary A communicates with owners of the targeted attribute based on its own choice. A may compromise certain user and obtain their attributes, where denotes the set of compromised users and denotes the whole user set, where

Step 2: A selects a target user, where users in own the targeted attribute.

Step 3: A generates by communicating with .

Step 4: The challenger selects , signs it and sends the ciphertext to A.

Step 5: A can choose to perform selection task any number of times and finally given out

A wins Game when .

Now define the following probabilities:

Thus, A wins the attribute detection game.

C. Adversary Model

The adversary thwarting the system can be classified into two categories according to the behaviors they conduct to obtain extra information: Semi-honest adversaries (or curious adversaries) are entities in the system that follow the protocol properly, with the only exception that an adversary may keep a record of all intermediate computation and communication in order to find extra information than intended for him. Malicious adversaries can deviate from the designated protocol, change their input, halt the protocol run before finishing and they will try to obtain the most extra information to other parties by providing false inputs. Assume that the user trusts the match selected to share his formation. Even if it is difficult to say the protocol is immune to malicious attacks completely, try to design protocols that defend malicious attacks, mention other related papers. In particular, the following adversary model are considered:

1) *Privacy inference from matching messages:* Getting users interests without getting caught for cheating unless they actually have the same interests.

2) *Brute-force Attack:* Exploring users' interests by including all likely or a large number of prevalent elements in their interest set. Allow users to create only a limited number of interests, maximum of ten.

3) *Impersonating other users:* ask each user to create a pair of asymmetric keys and use the hash value of the public key as their user ID. After two users meet, they first exchange their public keys, and they then negotiate a secret key using each other's public key. They can derive a session key using this secret key. This authenticates each partner of the protocol.

4) *Eavesdropping the communication between any two users:* Sensitive information is encrypted by the session key established by the two users.

D. Design Goal

The proposed privacy-preserving matchmaking protocol for mobile social networks should satisfy the following objectives.

1) *Privacy guarantee:* The proposed matchmaking protocol can preserve the user's privacy be they external or internal attackers.

2) *Security:* The proposed protocol's security should not be compromised.

3) *Efficiency:* The proposed protocol should be efficient.

IV. Design

Divide the protocol into three phases. Initial, Signing phase and Matchmaking phase. In the Initial Phase, Bob communicates his personal interest to the ID signer. Bob again sends to the ID signer a public Key after he generates a pair of RSA keys. The ID signer perform an identification, authentication and in turn issues a certificate to Bob. The certificate issued to Bob includes an RSA public Key and a user ID (note that the hash values of a user's RSA public Key is used as his or her USER ID.) The certificate issued by the ID signer is unique for each user. In the Signing phase, Bob makes known to the PIS his interest & user ID including the certificate issued by the ID signer. A verification is done to ensure that Bob does not misconduct himself which is based on other user's complaints. But in the case, presume that Bob has not misconducted himself and therefore he is a truthful user. Matchmaking phase to determine the common attributes using private set intersection and check whether it is above the threshold to select the match. Users then compute the secured channel to exchange attribute set with matchmaking. Lastly each user reports back to the PIS the attributes the other party used for matchmaking. Assume that users run a signature based authentication before the matchmaking starts.

A. *Security Assumptions*

These are some threats which are not considered in the system and some assumptions that are made:

- Users keep their private keys safe, so that malicious users could not steal their private keys to impersonate them.
- The third party server is not compromised by attackers.
- The parties participating in the protocol should learn about the size of the intersection set.
- In the protocol, assume that most users are rational and they are honest but curious. This means that most users are not going to reveal information if it brings them negative effects.
- Users trust that their matched friends will not disclose their matched information.
- Users will finish running the protocols once started.

B. *The protocol*

1. Let choose

Alice → **Bob**

2. Let and chooses

Bob → **Alice**

ce verify Bob Verifies **(**

Bob verify Alice Verifies **(**

If ok then go to next step **else** abort.

4. Alice computes ,
   Bob computes ,

5. **Alice** → **Bob**

6. **Bob** → **Alice**

If

7. (

Bob → **Alice**

8. **Alice** → **Bob**

In Step 1-3, Alice and Bob exchange their exponent values by running the DH session key negotiation and the corresponding signatures to ensure authencity of their values, Alice and Bob sign their messages to ensure non-repudiation in case of mishavior is detected later. In step 3, both parties verify the signatures if it fails the protocol is aborted else go to step 4. In step 5 and 6 Alice and Bob exchange the re-encrypted attributes in random order to Alice. Alice and Bob both compute the intersection set in step 6, both can only be sure of the number of common attributes in the intersection sets due to the random order of the re-encypted attributes they provide to each other. If the number of common attributes is greater than or equal to the minimum threshold required to find a friends both users calculate the session key else abort. In step 7 and 8, both users exchange the number of common attributes. Then the protocol comes to an end. Both the initiator and the canddidate must report to the PIS the attributes used by the other party for the friend discovery.

V. Analysis

A. *Security Analysis*

The security of this protocol holds if and only if RSA factorization and CDH assumptions holds. The attacks considered are whether an attacker can infer sensitive information from observing the protocol messages, whether the misbehavior from one of the parties would allow the other to learn any other interest either than the one they have in common and lastly whether one of the parties could prevent the other from leaking an interest that the two of them have in common. Assume that the IDS and PIS are trusted and it will not leak any information to other parties.

1) *Semi-honest users*

For an adversary who tries to infer the key or an encrypted attribute according to the property of DDH (Decisional Diffie-Hellman Hypothesis) it is impossible. For example Bob cannot map back to if he does not know the value of, which is known only to Alice. Also given the values of Bob cannot compute the value of.

2) *Malicious users*

For adversary who tries to infer useful information from uncommon interests if DDH [11] is hard. For example a malicious user tries to use attributes not signed by PIS. This is impassible since all users' attributes are signed by the PIS who is a trusted third party. Also, since each signed attribute is attached to the user identity it is impossible to use other users attributes or replay other responses hence avoids impersonation.

Lastly is not possible for any malicious user to learn all the common interest only the intersection set is known to both.

Table 1 shows the comparison of the protocol with two other encryption based protocols on threats below.

TABLE I. anti-attack capacity comparison

Protocols	*Semi-honest*	*Uncommon interest*	*Common interest*
Xie [8]	√	√	√
Agrawal's[7]	√	×	×
The Protocol	√	√	√

B. *Performance Analysis*

Simulate the protocol to see the overhead in terms of computation, communication and execution time. The computation and communication measures the resource consumption whiles the time of execution is measured from when the initiator starts until the initiator and the selected match exchange their actual attributes.

The computational and communicative cost of the protocol and that of Xie's is shown in Table 2. The Computational cost is evaluated using the number of Power Modular computation (PM), and the communicative cost is evaluated using number of messages transmitted. As it can be seen that the protocol has same computational cost with less communication cost hence less overhead cost compared to that of Xie's.

TABLE II. Comparison of Complexity

Protocols	*Computation cost*	*Communication cost*
Xie's	2(N-1)(m + n)PM+2(N-1)DH	(N-1)(m+n+5)
Our's	2(N-1)(m + n)PM+2(N-1)DH	(N-1)(m+n+3)

The simulation is build using RSA library in C. Choose a prime p of length 1024 bits and the RSA modulus (n) length of 1024 bits. The attribute size is 32 bits and each interest is 8 bits. Simulate the protocol on an Acer 4741g PC, which has Intel i3 at 2.5 GHz x 2 with 2G RAM.

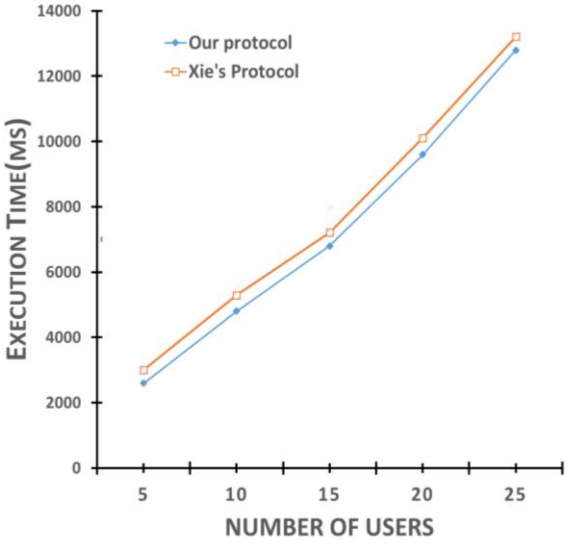

Figure 2. Execution time with increasing number of users

Fig.2 shows the comparison of the protocol to that of Xie's with increasing number of users but fixed size of attributes. A fixed attribute size of 10 is considered in this simulation. The protocol execution time is significantly less as compared to that of Xie's.

The protocol is more efficient as compared with that of Xie's as the communication cost is significantly reduce by 40 percent hence saves up to 40 percent of overhead cost. Our protocol is suitable for resource constraint mobile environment. Also the execution time is considerably reduced and therefore more efficient for matchmaking in MSN.

VI. Conclusion

In this paper, the proposed matchmaking protocol is able to offer fast and efficiency friend discovery with reduced steps and overhead. Reduce the steps involved in the process. Setup procedures are minimized, signature-based authentication and revocation procedures. The proposed protocol had reduced communicational complexity whilst maintaining the privacy of users. The protocol execution time is much less and also achieves Confidentiality, non-repudiation, privacy under the DDH hardness and RSA factorization and therefore suitable for privacy preservation in MSN.

Acknowledgment

This work is supported in part by the Applied Basic Research Programs of Science and Technology department of Sichuan Province (2015JY0043), the Postdoctoral Science Foundation of China (2013M542267), Open Research Foundation of Integrated Electronic System of the Ministry of Education of China (20120105), and the Fundamental Research Funds for the Central Universities (ZYGX2013J118, ZYGX2013J079).

References

[1] J. Ruiter and M. Warnier, Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice, Computers, Privacy and Data Protection: An Element of Choice, 2011 – Springer

[2] Zhu, Haojin, et al., Fairness-aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks. 1-1.

[3] N. Eagle and A. Pentland. "Social Serendipity: Mobilizing Social Software". IEEE Pervasive Computing, 4(2):28–34, 2005.

[4] A-K Pietil ̈ainen, E. Oliver, J. LeBrun, G. Varghese, and C. Diot. "Mobiclique: Middleware for Mobile Social Networking" In Proc. of WOSN'09

[5] M. Li, u, and W. Lou. "FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks", In Proc. of Infocom 2011.

[6] M. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in EUROCRYPT'04. Springer-Verlag, 2004, pp. 1–19

[7] L. Kissner and D. Song, "Privacy-preserving set operations," in CRYPTO '05, LNCS. Springer, 2005, pp. 241–257

[8] Y. Sang, H. Shen, and N. Xiong, "Efficient protocols for privacy preserving matching against distributed datasets", in ICICS '06. Springer-Verlag, 2006, pp. 210–227.]

[9] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in ISPEC'08, 2008, pp. 347–360

[10] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in ACNS '09, 2009, pp. 125–142

[11] R. Li and C. Wu, "An unconditionally secure protocol for multi-party set intersection," in ACNS '07, 2007, pp. 226–236

[12] G. S. Narayanan, T. Aishwarya, A. Agrawal, A. Patra, A. Choudhary, and C. P. Rangan, "Multi party distributed private matching, set disjointness and cardinality of set intersection with information theoretic security," in CANS '09. Springer - Verlag, Dec. 2009, pp. 21–40

[13] M. Shaneck and Y. Kim, "Efficient cryptographic primitives for private data mining," in HICSS '10, 2010, pp. 1–9

[14] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in TCC'08, 2008, pp. 155–175

[15] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 577–594

[16] E. D. Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in Financial Cryptography and Data Security '10, 2010

[17] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in SIGMOD '03. New York, NY, USA: ACM, 2003, pp. 86–97

[18] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining," J. Comput. Secur., vol. 13, no. 4, pp. 593–622, 2005

[19] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Serverless friend-of-friend detection in mobile social networking," in IEEE WIMOB '08, Oct. 2008, pp. 184 –189

[20] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in SIGMOD '03. New York, NY, USA: ACM, pp. 86–97, 2003

[21] Q. Xie, U. Hengartner. "Privacy-Preserving Matchmaking for Mobile Social Networking Secure Against Malicious Users", In Proc. 9th Int'l. Conf. on Privacy, Security (PST), and Trust 2011.

[22] N. Vastardis, and K. Yang, "Mobile Social Networks: Architectures, social properties, and key research challenges", IEEE, pp.1355 – 1371, 2012.

[23] Ansuura J. B. A. K, Xia Q. Klugah-Brown B., “Distributed Privacy preservation Matchmaking protocol in Mobile Social Network”, IJESI, vol 4 no. 5, pp 07-17, 2015.

[24] N. Kayastha, D. Niyato, P. Wang and E. Hossain, “Applications, Architectures, and protocol design issues for mobile social networks: A survey”, in vol. 99, No.12 December 2011|proceedings of the IEEE. Pp.2130 – 2158, 2011.

[25] D. Boneh, “The Decision Diffie-Hellman Problem”.