ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

ICMP: A Novel Profile Matching Scheme in Mobile Social Networks

[1]Prabhakara Rao Motan

M.Tech Student, Dept of CSE, St. Ann's College of Engineering & Technology, Chirala, Prakasam Dist, A.P, India

2 Dr. P. Harini

Professor and HOD Dept of CSE, St. Ann's College of Engineering & Technology, Chirala, Prakasam Dist, A.P, India

Abstract:

As the increasing use of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of peoples' lives. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However in this paper we create a profile matching application which helps user to find the people whose profile best matches with others people. In this paper we propose the security protocol which helps from profiling, and we have tried to increase the privacy so that less information about the user profile is revealed.

1. INTRODUCTION

A boom in mobile hand-held devices greatly enriches the social networking applications. Many social networking services are available on mobile phones (*e.g.*, JuiceCaster, MocoSpace and Wi-Fi Face [4]) and majority of them are location-aware (*e.g.*, FourSquare, BrightKite and Loopt). However, most of them are designed for facilitating people connections based on their real life social relationship [5], [6]. There is an increasing difficulty of befriending new people or communicating with strangers while protecting the privacy of real personal information. Friend and communication are two important basic functions of social networks. When people join social networks, they usually begin by creating a profile, and then interact with other users. Profile matching is a common and helpful way to make new friends with common interests or to search for experts [7]. Some applications help a user automatically find users with similar profile within a certain distance. For example, in the social network *Color*, people in close proximity (within 50 meters) can share photos automatically based on their similarity. MagnetU [1] matches one with nearby people for dating, friend-making. Small-talks [9] connect proximate users based on common interests. These applications use profiles to facilitate friend between proximate strangers and enable privacy preserving people searching to some extent.

Observe that in practice the mobile Internet connection may not always be available and it may incur high expense. Thus, in this work we focus on proximity-based decentralized mobile social networks (MSN) based on short-range wireless technologies such as Wi-Fi and Bluetooth. However the increasing privacy concern becomes a barrier for adopting MSN. People are unwilling to disclose personal profiles to arbitrary persons in physical proximity before deciding to interact with them. The insecure wireless communication channel and potentially untreated service provider increase the risk of revealing private information.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Friend based on *private profile matching* allows two users to match their personal profiles without disclosing them to each other. There are two mainstreams of approaches to solve this problem. The first category provides private attributes matching based on *private set intersection* (PSI) and *private cardinality of set intersection* (PCSI), [10], [8]. The second category measures the social proximity by *privatevector dot product* [2], [3],. They rely on public-key cryptosystem and homomorphism encryption, which results in expensive computation cost and usually requires a trusted third party. Multiple rounds of interactions are required to perform the presetting (*e.g.* exchange public keys) and private matching between each pair of users. Moreover, most protocols are *unverifiable*: there lack efficient methods to verify the result. Furthermore, in these approaches, matched users and unmatched users all get involved in the expensive computation and learn their matching results (*e.g.* profile intersection) with the initiator. These limitations hinder the adoption of the SMC related private matching methods in MSN.

A secure communication channel is equally important in MSN. Although the matching process is private, the following chatting may still be disclosed to the adversary and moreprivacy may be leaked. Most protocols assume that there isa secure communication channel established by using public keycryp to system. This involves a trusted third party and key management, which is difficult to manage in decentralized MSN.

Face-to-face interaction plays an irreplaceable role in our daily lives, especially for social networking purposes the initiator and its best matching user directly and privately find out and connect to each other, without knowing anything about other users' profile attributes, Making new connections according to personal preferences to matching users profile is the crucial task, while the rest of the users should also learn nothing about the two user's matching attributes. However in several applications, the users' personal profiles may contain sensitive information that they do not want to make public. In this paper, we propose a set of privacy-preserving profile matching schemes in MSN .We have defined several privacy levels for secure profile matching. However, it is challenging to find out the matching users privately while efficiently. Recently, Yang *et al*. proposed E-Small Talker which suffers from the dictionary attack which does not fully protect the non-match attributes between two users. We propose privacy-preserving profile matching schemes, known as private set intersection (PSI) protocol solutions based on existing PSI schemes are efficient.

2.PROFILE MATCHING TECHNIQUES

Profile matching is done through different techniques in different paper we go through it one by one

A. Honest but curious

In this paper [12] proposed by Mingle, Shushing yawning cao, winingLou the adversary is Honest but curious i.e. a participant will infer private information from protocol run but honestly follow the protocol. Will discuss how our protocols can be extended to achieve security in that model. The adversary may act alone or several parties may collude. We assume that the size of a coalition is smaller than a threshold *t*, where *t* is a parameter. Having different privacy level where PL-2(Privacy level) leaks less information.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

B. Shamir secret sharing based on SMC

Share of secret *s* under Shamir secret sharing (SS) scheme, [1] shares secret *s* among *w* parties by giving each party *Pi* the value [*s*]*it,w,* and if any at most *t* parties collude they cannot gain any information about *s*. Thus their protocol realizes randomization and degree-reduction in one round by letting each *Pi* pick a random *t*-degree polynomial and re-share $[\alpha]_i^{t,w}[\beta]_i^{t,w}$to others: Round 1. Each party *Pi* shares the value $[\alpha]_i^{t,w}[\beta]_i^{t,w}$by choosing a *t*-degree random polynomial *hi*(*x*), s. t. *hi*(0) =$[\alpha]_i^{t,w}[\beta]_i^{t,w}$. He sends the value *hi*(*j*) to party *Pj* , $1 \leq j \leq w$. Round 2: Every party *Pj* computes his share of $\alpha\beta$, i.e., the value *H*(*j*) = $[\alpha\ \beta]_j^{t,w}$under a *t*-degree random polynomial *H*, by locally computing the linear combination $H(j) = \Sigma^{w}_{i=1}$ $\lambda i hi(j)$, where $\lambda 1, \ldots, \lambda w$ are known constants. An additive homomorphism encryption scheme *E* allows one to compute *E*(*m*1+ *m*2) given *E*(*m*1) and *E*(*m*2), without knowing the plain texts. This is used in our protocol for PL-2.

C. Remainder Vector and Hint Matrix

The author Lan Zhang,Xiang-Yang [2] proposes this mechanism where search is not *flexible* The initiator cannot query any subset of other's profile. A perfect matching is required and *no fuzzy* search is supported. All participants decrypt the message. A *hint matrix* is constructed to support a flexible fuzzy search. It describes the linear constrain relationship among the optional attributes to help calculating unknown attributes from known attributes. The hint matrix helps a matching user exceeding the similarity threshold to recover the required profile vector.

a) Location Attribute and Its Privacy Protection

In localization enabled mobile social networks, a user usually searches matching users in vicinity. In the existing systems, a user is required to provide his/her own current location information and desired search range. The distance bound to define vicinity, if two users are within each other's vicinity, the intersection of their vicinity regions will have a proportion no less than a threshold. Compared to static attributes like identity information, location is usually a temporal privacy [2].

b) Privacy Preserving Profile Matching Protocols

In [2] Protocol 1, an unmatched relay user doesn't know anything about the request. The matching user knows the intersection of required profile and his/her own profile in the HBC model. A matching user can decide whether to reply the request according to the profile intersection. The initiator doesn't know anything about any participant until he/she gets a reply. To prevent malicious participants, we design Protocol 2, which is similar to Protocol 1, but it excludes the confirmation information from the encrypted message. To prevent the dictionary profiling by malicious initiator, we improve Protocol 2 to Protocol 3 which provides a user personal defined privacy protection.

D. Matchmaking Protocol

The paper proposed by Qi Xie and Urs Hengartner [14] illustrates several cryptographic protocols for matchmaking: In Initial phases the identity signer and a user guarantees that one user is assigned to only one identifier. Interest Signing Phase: This phase takes place between the personal interest signer (PIS)

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

and a user (e.g., Alice). The PIS generates a safe prime, p, the first time when it starts When a user creates a name for a new interest, the PIS chooses a quadratic residue modulo p as the id of this interest. Matchmaking Phase: Alice and Bob exchange their exponentiated values, as received from the PIS, and the corresponding signatures to ensure authenticity of these values. Alice and Bob sign their messages to ensure non-repudiation in case misbehavior is detected.

E. PRF and Oblivious PRF

In this paper Stainslaw Jarecki and Xiaomin Liu [15] Proposes Pseudorandom function (PRF) is an efficiently computable keyed function fk(.) whose values are indistinguishable, for a randomly chosen key k, the oblivious PRF is a protocol that allows the sender S on input key k, to let the receiver R compute the value fk(x) of a PRF fk(.) on any input x of R's choice without releasing any other information to R and do so obliviously in the sense that sender S learns nothing from the protocol similarly as in oblivious transfer or oblivious polynomial evaluation.

F. Secure Dot Product Protocol s

In this paper Wei Dong, Vacha Dave, ili Qiu, YinZhang [16] proposes Authentication and verification are essential to guard against malicious users who falsify the social coordinates, both parties to obtain the dot product, both Alice and Bob run two separate instances of protocol in parallel. Then, a naive verification approach for Bob may be to first decrypt the result sent by Alice using his private key and encrypt it using Alice's public key and compare it with w that he computed before for consistency. In protocol 0 Alice and bob start exchanging their encrypted vectors EH+A(v, r1) and EH+B(u, r2). Alice computes EH+B(v◦u, r2◦v) and EH+B(r1◦u, r1◦r2) and send them to Bob after self-blinding. Bob computes and sends back for self blinding. Alice decrypts and gets two numbers as result1 and result2. Alice computes and compares the vectors; if they are consistent the dot product result is correct.

TABLE 1 COMPARISION OF TECHNIQUES

Techniques	Attacks	Communication Cost	Computation Cost
Honest-but-curious	Active attacks	High	Less
Remainder Vector and Hint Matrix	Dictionary attack, man-in-the-middle	Average	Less
Matchmaking Protocol	Eavesdropping, impersonating	High	High
Dot product protocol	Denial-of-service, forgery	Less	High

3. RELATED WORK

Most previous private matching work is based on the secure multi-party computation (SMC) .There are two

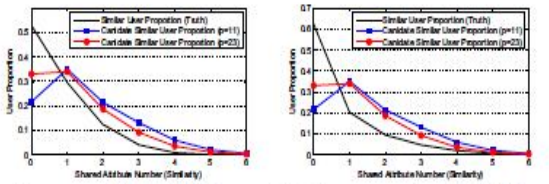

Fig.1.Candidate user proportion with different similarity and prime number.

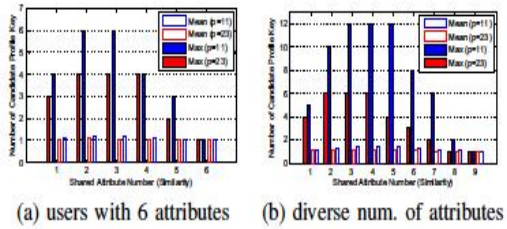

Fig. 2. Size of candidate profile key set with different similarities. Mainstreams of approaches to solve the private profile-based friend problem. The first

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

category is based on private stinted section (PSI) and private cardinality of set intersection (PCSI) [10], [8]. Early work in this category mainly addresses the private set operation problem in database research, *e.g.* [11]. [10], [8] provide well-designed protocols to privately match users' profiles based on PSI and PCSI. The second category is based on private vector dot product [3]. [2], [7] considers a user's profile as vector and use it to measure social proximity. A trusted central server is required to recomputeuser's social coordinates and generate certifications and keys. [11] Improves these work with a fine-grained private matching. However, in the PSI based schemes, any user can learn the profile intersection with any other user. The PCSI and dot product based approaches cannot support a precise specific profile matching's. These protocols often rely on public-key cryptosystem and/or homomorphism encryption which results in expensive computation cost and usually requires a trusted third party. Even unmatched users involve in the expensive computation. Furthermore, these protocols are unverifiable.

Secure communication channel construction is very important in practical private friend system but is often ignored. Secure communication channels are usually set up by authenticated key agreement protocols. This can be performed by relying on a public-key infrastructure, e.g., based on RSA or the Diffie-Hellman protocol.The public-key based methods allow parties to share authenticated information about each other, and however they need a trusted third party. Although Diffie-Hellman key exchange method allows two parties to jointly establish a shared secret key, it is known to be vulnerable to the Man-in-the-Middle attack. Device pairing is a technique to generate a common secret between two devices that shared no prior secrets with minimum or without additional hardware, . However, they employ some out-of-band secure channels to exchange authenticated information or leverage the ability of users to authenticate each other by visual and verbal contact. The interaction cost is not well suited to MSN where secure connections are needed immediately between any users. With these existing schemes, it is more complicated to establish a group key. Attribute based encryption is designed for access control of shared encrypted data stored in a server Only the user possessing a certain set of credentials or attributes is able to access data. All the ABE schemes rely on asymmetric-key cryptosystem, which cost expensive computation. And they require a complicate setup and a server.

4. CONCLUSION

In this paper we have surveyed different Profile Matching Techniques for mobile social network; we compared different technique based on their performance as we have studied in the papers. By surveying we have seen that the security of the profile of users is the major issue in profile matching in mobile social network, we have to implement the best technique which is less prone to attacks and requires less communication cost and computation cost.

REFERENCE

[1] "Magnetu," http://magnetu.com.

[2] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Proceedings of IEEE INFOCOM*, 2011.

[3] I. Ioannidis, A. Grama, and M. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in *Proceedingsof IEEE ICPP*, 2002.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 189-194 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

[4] L. Zhang, X. Ding, Z. Wan, M. Gu, and X. Li, "Wiface: A secure geosocial networking system using wifi-based multi-hop manet," in *ACMMobiSys MCS workshop*, 2010.

[5] K. Okamoto, W. Chen, and X.-Y. Li, "Ranking of closeness centrality for large-scale social networks," in *FAW*, 2008.

[6] S.-J. Tang, J. Yuan, X. Mao, X.-Y. Li, W. Chen, and G. Dai, "Relationship classification in large scale online social networks and its impact on information," in *Proceedings of IEEE INFOCOM*, 2011.

[7] L. Zhang, X.-Y. Li, J. Lei, J. Sun, Y. Liu, "Mechanism design for finding experts using locally constructed social referral web," in *TPDS*, 2013

[8] M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Serverless friend-of-friend detection in mobile social networking," in *Proceedings of IEEE WIMOB*, 2008.

[9] Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in *Proceedings of IEEE ICDCS*, 2010.

[10] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *Proceedings of IEEEINFOCOM*, 2011.

[11] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in *Proceedings of IEEEINFOCOM*, 2012.

[12] Ming Li, Shucheng Yu, "Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks"in IEEE 2013 VOL:12 NO:5.

[13] " Lan Zhang, Xiang-Yang li, Yunhao Liu "Message in a sealed Bottle: Privacy preserving Friending in Social Networks" in IEEE conference 2013 1063/6927.

[14] Qi Xie and Urs Hengartner ,"Privacy Preserving Matchmaking for mobile social networking secure against Malicious users" international conference 2011 978-1-4577-0584-7/11.

[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] Wei Dong, Vacha Dave , ili Qiu ,Yin Zhang "Secure Friend Discovery in Mobile Social Networks" in infocom 2011.

AUTHORS:

PrabhakaraRao Motan received the B.Tech degree in Computer Science & Engineering from JNTU Kakinada, in 2009 & pursuing her M.Tech in Computer Science & Engineering from JNTU Kakinada.

Dr. P. Harini is presently working as a professor and HOD,Dept of Computer Science and Engineering,in St.Ann's College of Engineering and Technology, Chirala.She obtained Ph.D in distributed and Mobile. Computing from JNTUA, nanthapur. She Guided Many UG and PG Students. She has More than 18Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded **Certificate of Merit** by JNTUK, Kakinada on the University Formation Day on 21 - August – 2012.