ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 384-390

Mobile Social Networks for Flattering Unsigned Profile Matching

[1] ANUSHA.V, [2] K.SUMALATHA

[1] M.Tech Research Scholar, Priyadarshini Institute of Technology and Science for Women
[2] Assistant Professor, Priyadarshini Institute of Technology and Science for Women

Abstract: Social networking makes digital communication technologies sharpening tools for extending the social circle of people. Privacy preservation is a significant research issue in social networking. Here user Profile matching with privacy preservation in mobile social networks (MSNs) is studied and a family of Profile matching protocols is introduced. An explicit Comparison-based Profile matching protocol (eCPM) which runs between two parties, an initiator and a responder is proposed which enables the initiator to obtain the comparison-based matching result about a specified attribute in their Profiles, while preventing their attribute values from disclosure. An implicit Comparison-based Profile matching protocol (iCPM) is then proposed which allows the initiator to directly obtain some messages instead of the comparison result from the responder. The messages unrelated to user Profile can be divided into multiple categories by the responder. The initiator implicitly chooses the interested category which is unknown to the responder. Two messages in each category are prepared by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute. iCPM is further generalized into an implicit Predicate-based Profile matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes.

Keywords: Mobile social network, Profile matching, privacy preservation, Homomorphic encryption, oblivious transfer

I. INTRODUCTION

Social networking is where individuals with similar interests connect with each other through their mobile/tablet. They form virtual communities. For example Face book, Twitter, LinkedIn etc. What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks. On many of the large SNSs, Participants are not necessarily "Networking" or looking to meet new people; instead they are primarily communicating with the people who are already part of their extended social network. To emphasize this articulated social network as a critical organizing feature of these sites, we label them "social network sites". Some web based SNSs support limited mobile interactions (e.g... Face book, MySpace and Cyworld).

Mobile Social Networks is a means of transmitting information (communicating) using a Mixture of voice and data devices over networks including cellular technology and elements of private and public IP infrastructure (such as the Internet). Mobile Social Networking'(MSN) refers to all of the enabling elements necessary for the contribution (posting 'and uploading) and consumption (viewing/experiencing) of social media across a mobile network. Key to the definition is the user's implicit or explicit choice of network technologies.

In the MSNs, we consider a generalized function to support information exchange by using Profile matching as a metric. Following the previous example, we consider two CIA agents with two different priority levels in the CIA system, A with a low priority l_A and B with a high priority l_B. They know each other as a CIA agent. However, they do not want to reveal their priority levels to each other. B wants to share some messages to A. The messages are not related to user

Profile, and they are divided into multiple categories, e.g., the messages related to different regions (New York or Beijing) in different years (2011 or 2012). *B* shares one message of a specified category at a time.

2. RELATED WORK

In general, the Profile matching can be categorized based on the formats of profiles and the types of matching operations. A well-known profile matching is the FNP scheme [19], where a client and a server compute their intersection set such that the client gets the result while the server learns nothing. Later, Kissner et al. [31] implemented profile matching with more operations including set intersection, union, cardinality and over-threshold operations. On the other hand, Ye et al. [32] further extended the FNP scheme to a distributed private matching scheme and Dachman-Soled et al. [33] aimed at reducing the protocol complexity. All the above solutions to the set intersection rely on homomorphic encryption operation. In the meantime, other works [34], [35] employed an oblivious pseudo random function to build their profile matching protocols, where communication and computational efficiency is improved. Li et al. [21] implemented profile matching according to three increasing privacy levels: i) revealing the common attribute set of the two users; ii) revealing the size of the common attribute set; and iii) revealing the size rank of the common attribute sets between a user and its neighbors. They considered an honest-but-curious (HBC) adversary model, which assumes that users try to learn more information than allowed by inferring from the profile matching results, but honestly following the protocol. They applied secure multi- party computation, the Shamir secret sharing scheme, and the homomorphic encryption scheme to achieve the confidentiality of user profiles.

The private matching schemes proposed in [2]–[4] aim at coarse-grained personal profiles and match two users based on a privacy-preserving computation of the intersection (cardinality) of their attribute sets. In contrast, our protocols support fine-grained personal profiles and thus much finer user differentiation, which is important for fostering the much wider use of PMSN. To our best knowledge, Dong et al. presented the only piece of work in [5] that does not match two users in PMSN using the intersection (cardinality) of their attribute sets. Instead, they proposed using the social proximity between two users as the matching metric, which measures the distance between their social coordinates with each being a vector precompiled by a trusted central server to represent the location of a user in an online social network. By comparison, our work does not rely on the affiliation of PMSN users with a single online social network and addresses a more general private matching problem for PMSN by supports fine-grained personal profiles and a wide spectrum of matching metrics.

In mobile social networking applications, profile matching acts as a critical initial step to help users, especially strangers, initialize conversation with each other in a distributed manner. Yang et al. [30] introduced a distributed mobile communication system, called E-Small Talker, which facilitates social networking in physical proximity. E- Small Talker automatically discovers and suggests common topics between users for easy conversation. Lu et al. [20] studied e-healthcare cases by proposing a symptom matching scheme for mobile health social networks. They considered that such matching scheme is valuable to the patients who have the same symptom to exchange their experiences, mutual support, and inspiration with each other.

The proposed profile matching protocols are novel since the comparison of attribute values is considered as the matching operation. The intuitive idea is inspired by the famous Yao's millionaires' problem [37] and its solution [40]. Similar to other works [21]–[23], we propose three different protocols with different anonymity levels. For the eCPM with conditional anonymity, we provide detailed anonymity analysis and show the relation

between pseudonym change and anonymity variation. For the iCPM and the iPPM with full anonymity, we show that the use of these protocols does not affect user anonymity level and users are able to completely preserve their privacy.

3. PROFILE MATCHING:

Profile matching means two users comparing their personal profiles and is often the first step towards effective PMSN. It, however, conflicts with users' growing privacy concerns about disclosing their personal profiles to complete strangers before deciding to interact with them.

3.1 Matching user profiles on social networks suffers currently of three main problems:

Social Network Representations:

Social network offer to users interesting means and ways to connect communicate and share information with other members within their platforms. However those sites have currently different structures/schemas and they represent users' profiles differently. Thus, they prohibit the exchange of information and communication with functioning as "Data Isolated Islands".

User Profile Domains:

Even when sites share the same representation, user profile attribute domains are not always common. For instance, the domain values of interests attribute in face book do not necessarily meet the domain values of the same attribute in LinkedIn.

Site/User Objective:

Depending on the site and on the user objectives, the same attribute can be filled up with two different values. For instance, the email attribute in face book is commonly filled with a personal email while LinkedIn one is assigned to the professional email of the same user.

3.2 User Profile Matching in Social Networks

Inter social network operations and functionalities are required in several scenarios (data integration, data enrichment, information retrieval etc...). To achieve this, matching user profiles is required. Profile Matching can be done using following components.

Components

FOAF (Friend of a Friend): is admitted to be one of the real success stories of the semantics web and is becoming a de facto standard with more and more social networks and tools that allow create/generate FOAF profiles.

Similarity Function Assignment: Comparing two profiles comes down to compare (a set of) their attributes. In order to obtain appropriate results, adapted similarity functions must be associated to each attribute (e.g.., comparing emails must be computed in a different way than comparing interests). Various techniques can be used to measure the similarities score between two textual/string values.Attribute Weight Assignment: This component mainly aims to assign a weight to each attribute in the FOAF vocabulary. This allows representing the attribute importance within a defined context. In this framework, the weight can be assigned manually or computed automatically.

Profile Matcher: This component aims to provide a decision whether two input profiles refer to the same physical person or not. Here, two profiles are considered as representing the same user if their profile similarity score is higher than a threshold called the profile matching threshold.

Acquiring the Data: To match user profiles from different OSN sites, a large and suitable dataset from social networks is required [12]. The data on the profile pages is retrieved using a crawler. The data on social networking sites can be very diverse, unstructured, and

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 384-390

even unsuitable, thus it will need pre-processing. Based on the knowledge of the structure of the user profile page and the user's friends' page in a particular network, content can be extracted. Then, irrelevant data can be filtered out.

Vector Space Model: In the vector space model, both documents and profiles are represented as vectors with components for different terms (term vectors) [12]. These components are weights that reflect the frequency of each term in the document and interest in a given term in the profile, respectively

4. EXPLICIT COMPARISON BASED APPROACH

eCPM protocol allows two users to compare their attribute values on a specified attribute without disclosing the values to each other. But, the protocol reveals the comparison result to the initiator, and therefore offers conditional anonymity. The protocol has a fundamental bootstrapping phase, where the TCA generates all system parameters, user pseudonyms, and keying materials.

A. Bootstrapping

The protocol has a fundamental bootstrapping phase, where the TCA generates all system parameters, user pseudonyms, and keying materials. Specifically, the TCA runs G to generate ⟨ p, q,R,Rq,Rp, χ⟩ for initiating the homomorphic encryption The TCA generates a pair of public and private keys (pkTCA, skTCA) for itself. The public key pkTCA is open to all users; the private key skTCA is a secret which will be used to issue certificates for user pseudonyms and keying materials, as shown below. The TCA generates disjoint sets of pseudonyms (pidi) and disjoint sets of homomorphic public keys (pki) for users (ui). For every pidi and pki of ui, the TCA generates the corresponding secret keys pski and ski. In correspondence to each pseudonym pidi, it assigns a certificate certpidi to ui, which can be used to confirm the validity of pidi. Generally, the TCA uses skTCA to generate a signature on pidi and pki. The TCA outputs certpidi as a tuple (pki, SignskTCA(pidi,pki)). The homomorphic secret key ski is delivered to ui together with pski; pki is tied to pidi and varies as the change of pseudonyms.

5. IMPLICIT COMPARISON BASED APPROACH

Here the implicit–based profile matching (iCPM) is proposed by adopting the oblivious transfer cryptographic technique. It is considered that users have distinct values for any given attribute. The iCPM consists of three main steps. Then encrypt the vector by using the homomorphic encryption and sends the encrypted vector but still can process on the cipher text. In the second step, computes the cipher texts with input of self-defined messages for 1 ≤message ≤length.

A. Protocol Steps

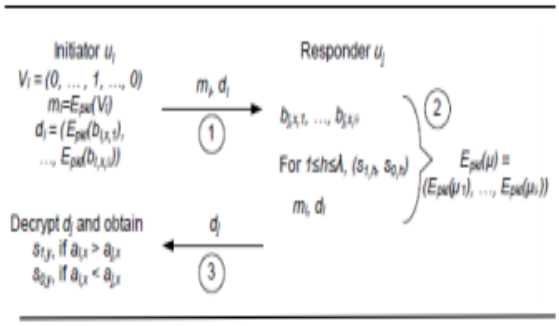

Fig 1. ICPM flow

6. PERFORMANCE ANALYSIS

The performance of three proposed protocols eCPM, iCPM, and iPPM is studied in terms of communication overhead and anonymity strength. When analyzing anonymity, it is considered that users have distinct values for any given attribute. Non-distinct attribute values and comparison operations —≥‖ and —≤‖ will be considered in the future work.

A. Communication Overhead

Let |R| be the size of one ring element in Rq. In the eCPM, the initiator and the responder both need to send cipher texts in size of 2|R| and the communication overhead is thus subject only to the system parameter |R|. In order to achieve full anonymity, the iCPM constructs cipher text in a sequence of operations. It is known that |Enc (b)| = 2|R|. Thus, the communication overhead of the initiator is $2(\theta + \lambda)|R|$ with $\theta = \log l$. It can be seen that the initiator's communication overhead increases with system parameters (θ, λ). An addition operation of homomorphic encryption does not increase the cipher text size, while a multiplication with inputs of two ciphertexts of lengths a|R| and b|R| outputs a (a+b−1)|R|-length cipher text. Thus, in the iCPM, the communication overhead of the responder increases to $6\theta|R|$. It is concluded that the communication overhead of the eCPM and the iCPM are constantly dependent on system parameters (θ, λ). The iPPM extends the iCPM by building complex predicates. From the protocol description, we observe that if a predicate includes $n \geq 1$ comparisons, the communication overhead of the iPPM would be approximately n times of that in the iCPM.

B. Anonymity

Suppose that user ui is currently using pseudonym pidi to execute profile matching with others. An adversary aiming to break the k-anonymity of ui is considered [11]. K-anonymity is a classic concept for evaluating anonymity. It implies that a series of comparison results provide k-anonymity protection to a user if the user's behavior cannot be distinguished from at least k − 1 other users.

7. CONCLUSION

A unique comparison-based profile matching problem in Mobile Social Networks (MSNs) has been investigated, and novel protocols are proposed to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional anonymity. It reveals the comparison result to the initiator. Considering the k-anonymity as a user requirement; the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs is analyzed. Further an enhanced version of the eCPM, i.e., eCPM+ is introduced, by exploiting the prediction-based strategy and adopting the pre-adaptive pseudonym change. The effectiveness of the eCPM+ is validated through extensive simulations using real-trace data. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) has been devised. The iCPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression made of multiple comparisons spanning multiple attributes. The iCPM and the iPPM both enable users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile information. In current version of the iCPM and the iPPM, —>‖ and —<‖ operations for profile matching is implemented.

REFERENCES

[1]"Comscore," http://www.comscoredatamine.com/.

[2] A. G. Miklas, K. K. Gollu, K. K. W. Chan, S. Saroiu, P. K. Gummadi, and E. de Lara, "Exploiting social interactions in mobile systems," in Ubicomp, 2007, pp. 409–428.

[3] S. Ioannidis, A. Chaintreau, and L. Massouli´e, "Optimal and scalable distribution of content updates over a mobile social network," in Proc. IEEE INFOCOM, 2009, pp. 1422–1430.

[4] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 632–640.

[5] W. He, Y. Huang, K. Nahrstedt, and B. Wu, "Message propagation in ad- hoc-based proximity mobile social networks," in PERCOM workshops, 2010, pp. 141–146.

[6] D. Niyato, P. Wang, W. Saad, and A. Hjørungnes, "Controlled coalitional games for cooperative mobile

social networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1812–1824, 2011.
[7] M. Motani, V. Srinivasan, and P. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in MobiCom, 2005, pp. 243–257.
[8] M. Brereton, P. Roe, M. Foth, J. M. Bunker, and L. Buys, "Designing participation in agile ridesharing with mobile social software," in OZCHI, 2009, pp. 257–260.
[9] E.Bulut and B.Szymanski, "Exploiting friendship relations for efficient routing in delay tolerant mobile social networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2254–2265, 2012.
[10] 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 ICDCS, 2010, pp. 468–477.
[11] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 857–865.
[12] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Morality- driven data forwarding with privacy preservation in mobile social networks," IEEE Transactions on Vehicular Technology, vol. 7, no. 61, pp. 3209–3222, 2012.
[13] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, 2005, pp. 71–80.
[14] F. Stutzman, "An evaluation of identity-sharing behavior in social network communities." iDMAa Journal, vol. 3, no. 1, pp. 10–18, 2006.
[15] K. P. N. Puttaswamy, A. Sala, and B. Y. Zhao, "Starclique: guaranteeing user privacy in social networks against intersection attacks," in CoNEXT, 2009, pp. 157–168.
[16] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in WWW, 2009, pp. 531–540.
[17] G. Chen and F. Rahman, "Analyzing privacy designs of mobile social networking applications," IEEE/IFIP International Conference on Em- bedded and Ubiquitous Computing, vol. 2, pp. 83–88, 2008. [18] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.- C. Wong, "Secret handshakes from pairing-based key agreements," in IEEE Symposium on Security and Privacy, 2003, pp. 180–196. [19] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in EUROCRYPT, 2004, pp. 1–19.
[20] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for healthcare social network," ACM Mobile Networks and Applications (MONET), vol. 16, no. 6, pp. 683–694, 2011.
[21] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 2435–2443.
[22] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc. IEEE INFO- COM, 2012, pp. 1969–1977.
[23] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 1647– 1655.
[24] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non- cooperative location privacy: a game-theoretic analysis," in ACM CCS, 2009, pp. 324–337.
[25] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86 – 96, 2011.
[26] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting dis- junctions, polynomial equations, and inner products," in EUROCRYPT, 2008, pp. 146–162.
[27] N. Eagle and A. Pentland, "Social serendipity: mobilizing social soft- ware," IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.
[28] J. Teng, B. Zhang, X. Li, X. Bai, and D. Xuan, "E-shadow: Lubricating social interaction using mobile phones," in ICDCS, 2011, pp. 909–918.

[29] B. Han and A. Srinivasan, "Your friends have more friends than you do: identifying influential mobile users through random walks," in MobiHoc, 2012, pp. 5–14.
[30] 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 ICDCS, 2010, pp. 468–477.
[31] L. Kissner and D. X. Song, "Privacy-preserving set operations," in CRYPTO, 2005, pp. 241–257. [32] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in ISPEC, 2008, pp. 347–360.
[33] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in ACNS, 2009, pp. 125–142.
[34] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC, 2009, pp. 577–594.
[35] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," Journal of Cryptology, vol. 23, no. 3, pp. 422–456, 2010.
[36] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik¨ainen, "On private scalar product computation for privacy-preserving data mining," in ICISC, 2004, pp. 104–120.