www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9333-9337

Matching Anonymized User Profiles In Mobile Social Networks

***M. Harini*[1], *M.Srilakshmi*[2], *Dr. S.PremKumar*[3]**

[1]M.Tech Student,
CSE Department,
GPCET(affiliated to JNTUA , Anantapur),
Kurnool, India
mharini30@gmail.com

[2] Assistant Professor,
CSE Department,
GPCET(affiliated to JNTUA , Anantapur),
Kurnool, India
marri_srilakshmi67@yahoo.co.in

[3] Professor and Head Of the Department,
GPCET(affiliated to JNTUA , Anantapur),
Kurnool, India
spkknl@gmail.com

Abstract: ***In this project, we try to study user profile matching with privacy-preservation in mobile social networks (MSNs) and introduce new type profile matching protocols. We first propose an explicit Comparison-based Profile Matching protocol (eCPM) that runs between two parties, a leader who initiates the communication and a communicator who responds. The eCPM permits the leader to get the result of attribute comparision between their profiles, while preventing their attribute values disclosure. We then propose implicit Comparison-based Profile Matching protocol (iCPM) that permits the leader to directly get some messages rather than the comparison result from the communicator. The messages unrelated to user profile are often divided into multiple classes by the communicator. The leader implicitly chooses the interested class that is unknown to the communicator.***

Two messages per each class are prepared by the communicator, and just one message is often obtained by the leader as per the result of comparison on the candidate attribute. We additionally generalize the iCPM to permit complicated comparison criteria spanning multiple attributes as implicit Predicate-based Profile Matching protocol (iPPM). eCPM reveals the comparision result to the leader and provides only conditional anonymity while iCPM provides full anonymity. We enhance eCPM, referred to as eCPM+, by combining the eCPM with a unique prediction-based adaptive anonym amendment strategy.

Key words: Mobile social network, user profile matching, privacy preservation, homomorphic encryption, oblivious transfer

1 INTRODUCTION

In social networking electronic communication technologies enhance the social relations of individuals. The ubiquitous adoption of the advanced hand-held devices and also the pervasive connections of Bluetooth/WiFi/GSM/LTE networks kindled the Mobile Social Networks (MSNs). In the MSNs, users can surf the net and even communicate with users in neighborhood through short-range wireless communications [1]–[3]. Owing to its geographical nature, the MSNs can handle several new applications [2]–[6]. For example, through Bluetooth communications, PeopleNet [2] permits cost-effective data search among mobile phones in close vicinity; a message-relay technique is usually suitable for carpool and ride sharing in a local region. By the discovery of latent merits of MSNs, recent analysis efforts have been focused on how to improve the efficacy and potency of the MSN communications. Specialized data routing and forwarding protocols that take various social features exhibited by users in MSNs such as, social relationship [3], social selfishness [5], and social morality [6] into account are used. A positive aspect is that the customary solutions can be extended to unravel the MSN issues by considering the distinctive social options.

Personal information is shared in social networks where privacy violation can take place easily [4] - [7]. Identity presentation and privacy terms are key issues that are to be addressed well [10], [11],[14]. Extension of social networking to mobile environment necessitates extensive privacy preservation to user identity because the neighbors in their immediate surroundings are not known to the users. Malicious nodes exist in MSNs who may intrude and store the personal information of other users in the MSN to correlate it at different times with location information. This can disclose the user's behavior. According to various surveys, many Social Networking Applications like neighborhood exploring and content sharing ones lack feedback or control techniques and hence disclose the personal information related to the users in MSNs. To overcome various privacy violation problems in MSNs, many privacy enhancing techniques have been employed [2], [9], [14] – [20].

For instance, when two strangers encounter in an MSN, privacy-preserving profile matching assists users to initialize speech with one another in a distributed and privacy-preserving manner. Several analysis efforts on the privacy conserving profile matching have been disbursed with a common goal of enabling the acknowledgment between two encountered users if both the users satisfy each other's criteria while eliminating the needless information speech act if they do not. The original initiative is associating an agent of the Central Intelligence Agency (CIA) to a server, without revealing her independent agency credentials unless the server is a real independent agency outlet. Also, the server need not reveal its independent agency credentials to anyone other than the independent agents. A similar example is illustrated in Fig.1.

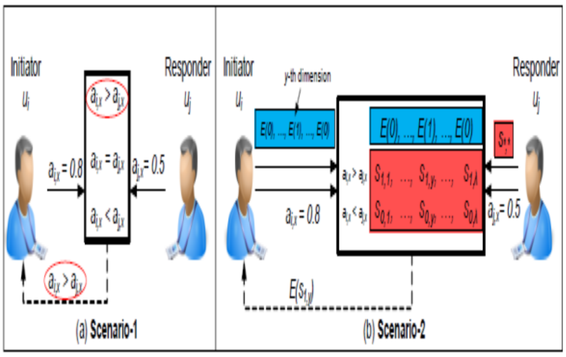

Fig.1 Profile Matching Between Leader And Communicator

1.1 The Problem

There are many privacy-preserving profile matching protocols [10], [20]–[23] which consider the overall similarity between two user profiles instead of specific attribute relation. They usually check whether the proximity level of the two profiles is larger, equal, or smaller than a pre-defined threshold parameter value. The proximity measurement shows the extent of intersection of two sets or the distance of two vectors where sets and vectors represent user profiles. Moreover, the profile matching results are delivered to the users who take part in communication making behavior linkage possible if the results are unique.

1.2 Model Of The Network

A consistent MSN comprising of N mobile users with the same range of bi-directional wireless communication is considered. The multi-pseudonym technique [21], [22] is adopted to preserve user identity and site privacy, where users make use of pseudonyms as their identities throughout the communication, altering them periodically. A Trusted Central Authority

(TCA) that generates profiles, pseudonyms and associated certificates for each and every user is employed for bootstrapping which is however not concerned in user communication.

2 RELATED WORK

Profile matching is the prominent communication option among users in MSNs in a distributed manner. Various efforts were put on this aspect giving rise to several techniques like E-SmallTalker for social networking in physical proximity, symptom matching scheme for mobile health social systems, e.t.c. Profile matching is usually based on the profile format and the type of matching operations. Popularly used such a scheme is FNP which was later enhanced reducing complexity. The employed profile matching protocols are new and use the comparision result for matching [23], [24]. The three proposed protocols provide anonymity to user profiles at three different levels, viz., eCPM ensures conditional anonymity while full anonymity is achieved through iCPM and iPPM respectively.

2.1 Primitives

The proposed protocols employ

2.1.1 Homomorphic Encryption

Homomorphic encryption schemes allow different computational operations like addition and multiplication on ciphertexts. They help users to manipulate with the encrypted original text even without the knowledge of the secret keys. These homomorphic encoding schemes are widely employed in knowledge aggregation and computation especially for privacy-sensitive content. Homomorphic encryption is the backbone of the proposed protocols.

2.1.2 Oblivious Transfer

Oblivious Transfer is the cryptographic technique in which receiver obtains a piece of information from many at the sender but the sender does not know which piece is received by the receiver. This scheme is used in iCPM and iPPM protocols.

2.2 Explicit Comparison Based Protocol

This protocol runs between the leader and the communicator and compares the values of a specified attribute. The values of attribute are not publicized but the result of comparision is delivered to the leader. Hence it confirms only conditional anonymity.

2.2.1 Bootstrapping

A Trusted Central Authority (TCA) is used to generate user pseudonyms, system parameters and other keying materials. TCA generates a pair of public and private keys for itself and also the function necessary to initiate the key technique, homomorphic encryption. TCA generates user ids, signatures, homomorphic public keys and corresponding private keys for all the users.

2.2.2 Protocol Steps

The leader sends its encrypted value of the candidate attribute to the communicator. The communicator checks the validity of the message received and then encrypts its own attribute value and calculates the comparision of the two values. Then the result is sent in encrypted form to the leader. The leader also verifies the validity of the message and then decrypts the result.

2.3 Implicit Comparison Based Protocol

This protocol follows oblivious transfer technique. The essential assumption is that the values of the attributes of the users in the MSN are distinct. The leader l_i selects the category it is interested in as T_y by setting the y^{th} element to 1 and other elements to 0 in λ-length vector V_i representing the category. The leader encrypts the vector using homomorphic encryption and forwards it to the communicator, u_j. Communicator doesn't know the value but processes it by using homomorphic encryption techniques. Then u_j computes the ciphertexts with input of self-defined messages ($s_{1;h}$, $s_{0;h}$) for $1 \le h \le \lambda$, two encrypted vectors (m_i, d_i) and its own attribute value $a_{j;x}$. In the last step, u_i decrypts the ciphertext and obtains $s_{1;y}$ if $a_{i;x} > a_{j;x}$ or $s_{0;y}$ if $a_{i;x}$

$< a_{j;x}$. Various steps involved in iCPM are illustrated in Fig.2.

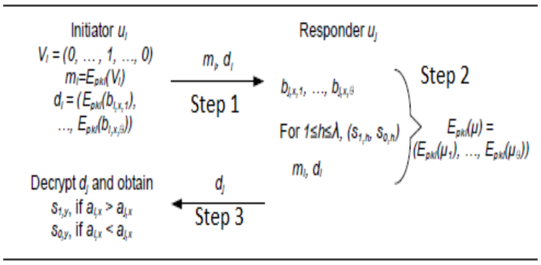
Initiator u_i
$V_i = (0, \ldots, 1, \ldots, 0)$
$m_i = E_{pki}(V_i)$
$d_i = (E_{pki}(b_{i,x,1}), \ldots, E_{pki}(b_{i,x,\theta}))$
m_i, d_i
Step 1
Responder u_j
$b_{j,x,1}, \ldots, b_{j,x,\theta}$
For $1 \leq h \leq \lambda$, $(s_{1,h}, s_{0,h})$
m_i, d_i
Step 2
$E_{pki}(\mu) = (E_{pki}(\mu_1), \ldots, E_{pki}(\mu_\theta))$
Decrypt d_j and obtain
$s_{1,y}$, if $a_{i,x} > a_{j,x}$
$s_{0,y}$, if $a_{i,x} < a_{j,x}$
d_j
Step 3

Fig.2 Steps In iCPM

2.4 Implicit Predicate Based Protocol

The previously discussed protocols compare the values of only one attribute at a time which complicates the comparision of multiple attribute values. Hence iCPM is extended to span multi attribute comparision criteria as a predicate without compromising the anonymity of the protocol. This is referred to as implicit predicate-based profile matching approach. The predicate is a logical expression containing multiple comparisions of different attributes and paves path for advanced matching criteria within a single run.

In the first step, different from the iCPM, u_i sends to u_j n encrypted vectors of its attribute values corresponding to the attributes in A where A ($|A| = n \leq w$) is the attribute set of the predicate Π. In the second step, u_j sets 2λ polynomial functions $f_{sat;h}(x)$, $f_{unsat;h}(x)$ for $1 \leq h \leq \lambda$. u_j then generates $2\lambda n$ secret shares from $f_{sat;h}(x)$, $f_{unsat;h}(x)$ by choosing $1 \leq h \leq \lambda$, $1 \leq x \leq n$, and arranges them in a certain structure according to the predicate Π. For every 2λ secret shares with the same index h, similar to the step 2 of the iCPM, u_j generates θ ciphertexts. u_j obtains $n\theta$ ciphertexts at the end of the second step. In the third step, u_i decrypts these $n\theta$ ciphertexts and finds n secret shares of $s_{1;y}$ and $s_{0;y}$. u_j finally can obtain $s_{1;y}$ or $s_{0;y}$ from the secret shares. The iPPM is obtained by combining the iCPM with a secret sharing scheme [25] to support a predicate matching. Various steps involved in iPPM are shown in Fig.3.

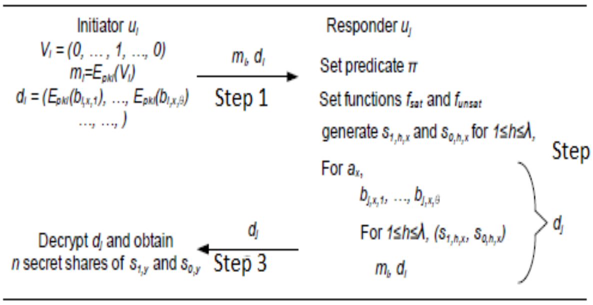
Initiator u_i
$V_i = (0, \ldots, 1, \ldots, 0)$
$m_i = E_{pki}(V_i)$
$d_i = (E_{pki}(b_{i,x,1}), \ldots, E_{pki}(b_{i,x,\theta}) \ldots, \ldots,)$
m_i, d_i
Step 1
Responder u_j
Set predicate π
Set functions f_{sat} and f_{unsat}
generate $s_{1,h,x}$ and $s_{0,h,x}$ for $1 \leq h \leq \lambda$,
Step
For a_x,
$b_{j,x,1}, \ldots, b_{j,x,\theta}$
For $1 \leq h \leq \lambda$, $(s_{1,h,x}, s_{0,h,x})$
m_i, d_i
d_j
Decrypt d_j and obtain
n secret shares of $s_{1,y}$ and $s_{0,y}$
Step 3

Fig.3 Steps In iPPM

3. CONCLUSION

Novel protocols are proposed for solving the special comparision-based profile matching drawback. Explicit Comparision-based Profile Matching (eCPM) protocol provides conditional namelessness by revealing the comparison result to the leader. Two protocols with full namelessness, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) are devised. iCPM compares the values of single attribute while iPPM spans multiple attribute comparision. iCPM and iPPM provide full namelessness. Proposed protocols, iCPM and iPPM implement profile matching using "$>$" and "$<$" operations. A possible future work is to increase them to support additional operations like "$\geq$" and "$\leq$". Another future work is to cover the predicate data within the iPPM. The present work may reveal the partial information related to the leader's interest.

4. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] M. Motani, V. Srinivasan, and P. Nuggehalli, “Peoplenet: engineering a wireless virtual social network,” in MobiCom, 2005, pp. 243–257.

[5] 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.

[6] 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.

[7] 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.

[8] Q. Li, S. Zhu, and G. Cao, “Routing in socially selfish delay tolerant networks,” in *Proc. IEEE INFOCOM*, 2010, pp. 857–865.

[9] 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.

[10] R. Gross, A. Acquisti, and H. J. H. III, “Information revelation and privacy in online social networks,” in *WPES*, 2005, pp. 71–80.

[11] F. Stutzman, “An evaluation of identity-sharing behavior in social network communities.” *iDMAa Journal*, vol. 3, no. 1, pp. 10–18, 2006.

[12] 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.

[13] 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.

[14] G. Chen and F. Rahman, “Analyzing privacy designs of mobile social networking applications,” *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2, pp. 83–88, 2008.

[15] 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.

[16] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in *EUROCRYPT*, 2004, pp. 1–19.

[17] R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mhealthcare social network,” *ACM Mobile Networks and Applications (MONET)*, vol. 16, no. 6, pp. 683–694, 2011.

[18] 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.

[19] R. Zhang, Y. Zhang, J. Sun, and G. Yan, “Fine-grained private matching for proximity-based mobile social networking,” in *Proc. IEEE INFOCOM*, 2012, pp. 1969–1977.

[20] W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in *Proc. IEEE INFOCOM*, 2011, pp. 1647– 1655.

[21] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, “On noncooperative location privacy: a game-theoretic analysis,” in *ACM CCS*, 2009, pp. 324–337.

[22] 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.

[23] A. C.-C. Yao, “Protocols for secure computations (extended abstract),” in *FOCS*, 1982, pp. 160–164.

[24] I. F. Blake and V. Kolesnikov, “Strong conditional oblivious transfer and computing on intervals,” in *ASIACRYPT*, 2004, pp. 515–529.

[25] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.