A New Privacy Preserving Private Profile Matching Technique for Proximity-based Mobile Social Networks

Konakanchi.V.S.H.Ganesh #1, Venkata Ramana Adari *2
[#1]M.Tech Scholar, [*2] Professor & HOD
Department of Computer Science & Engineering,
Vizag Institute of Technology Engineering College,
Dakamarri, Visakhapatnam Dist, AP, India.

Abstract

Mobile adhoc social networks are mainly represented as self configuring social networks, which connect users using various mobile devices, such as laptops, PDAs, and cellular phones. The information which is available in Social network is now being used in ways for which it may have not been originally intended. In existing systems for creating profile matching services, usually all the users directly publish their complete profile information for others to search. However, in many online applications, the users' personal profiles may maximum contain their own sensitive and valuable information which they don't want to make it public. However, current models for inter changing their personal information require users to compromise their privacy and security. We now present several of these privacy and security issues, along with our design and implementation of solutions for these issues. In this paper, we propose a new FindU model, a set of privacy-preserving profile matching schemes for proximity-based mobile social networks. In FindU model, an initiating user can find from a group of users the one whose profile best matches with his/her profile, where they can interchange only useful information and to limit the risk of privacy exposure.

Keywords

Proximity-based Mobile Social Networking, Profile Matching, Mobile Adhoc Network, Security, Privacy.

1. Introduction

Social Network Sites (SNS) are recently becoming a very popular platform for interacting and communicating amongst individuals and groups. As there was tremendous popularity of various portable mobile devices such as smart phones, phones and tablets are focusing the emergence of proximity-based mobile social networking (PMSN), which refers to adjacent mobile users interacting through the Bluetooth/ Wi-Fi interfaces on their individual mobile devices. In contrast to traditional web-based online social networking, PMSN can enable more tangible face-to-face social interactions in public places such as parks, stadiums, and cinema theatres, railway stations.

Furthermore, online social network information is now being collectively combined with users' physical locations like handheld devices, allowing information about users' preferences and social relationships to interact in real-time with their physical environment, which is shown clearly in figure 1. The integrated fusion of online social networks with real-world mobile computing [1] has created a fast growing set of applications that have unique requirements and unique implications that are not yet fully understood. For example, MagnetU and E-SmallTalker [2] are most widely used MSN applications that match one with nearby people for dating or friend-making based on common interests. For such a type of applications the user is intended to give an input query with any one of attribute in his/her profile, and the system would automatically find the nearest matched profile around various people with same similar profile matching. The scope of these applications are very broad, since people can input anything as they want, such as hobbies, phone contacts and places they have been to. The latter can even be used to find “lost connections” and “familiar strangers” which is shown in figure 2.

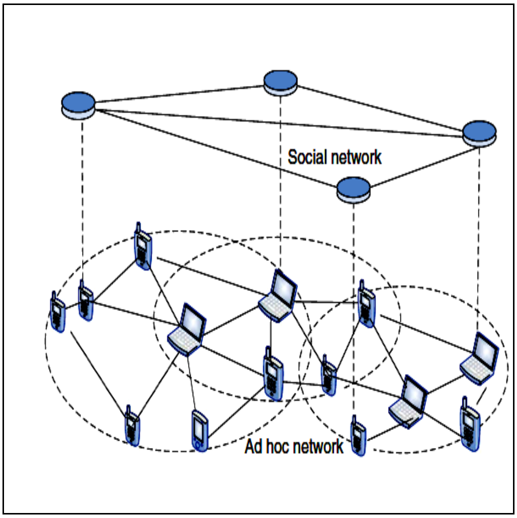

Fig.1. System Overview

In this paper, we try to overcome the above challenges and make the following main contributions

(1) We formulate the privacy preservation problem of profile matching in MSN. We totally formulated two levels of privacy which was defined along with their threat models, where the higher privacy level explodes less profile information to the adversary than the lower privacy level.

(2) We also proposed two fully distributed privacy-preserving profile matching schemes, one of them being a private set intersection (PSI) protocol and the other is a private cardinality of set-intersection (PCSI) protocol.

(3) We also provide formal security proofs and extensive performance evaluation for our schemes. Our two protocols are shown to be secure under the honest-but-curious (HBC) model, with information-theoretic security (for PSI) and standard security (for PCSI), respectively.

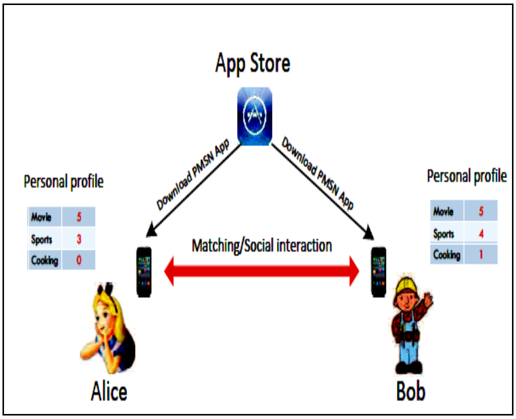

Fig. 2: Illustration of proximity-based mobile social networking and profile matching.

2. Background Work

In this section we mainly provide the short introduction to work in the area of mobile social networking and the technologies that have made it possible.

I. Mobile Computing

For the very growing third-party application developers the smart phones are now becoming very useful for a lot of internet users to be connected with each other. This Mobile computing has made the users to get the power of personal computing in their pockets by giving them ubiquitous access to rich online social network information. In certain areas (such as college, university campuses) there are now high concentrations of active social network users with Smartphone’s. Recently there was a tremendous increase of users who use the smart phones which have inbuilt internet access and Wi-Fi support for supporting the development of third-party applications. In fact, according to Net Applications, Apple's handheld status symbol accounted for nearly two-thirds of all mobile web browsing traffic in April of 2009, almost nine times more than the nearest competitors [3].

II. Social Networks

The tremendous growth of online social networks has drastically increased during these years. In particular, the most fascinating application in online social networking sites is Facebook, which has spread internationally and to users of a wide age range. According to Facebook.com's introduction statistics page, the site has over 300 million active users [4], [5], of which over 200 million log on every day.Inorder to compare the active users score with Com Score's global Internet usage statistics [6], this would simply tell that nearly 10 in 100 of all Internet users log on to Facebook everyday and that the active Facebook Internet population is larger than any single country's Internet population. Out of those all the users count, mobile users in particular are active Facebook users. According to Facebook statistics which was done in the year of March 2009, there are currently over 30 million active mobile users of Facebook, and those users are almost 50% more active on Facebook than non-mobile users.

3. Problem Formulation

This Section mainly deals with three various concepts. They were discussed in detail in this section.

A. Proximity-based Mobile Social Networking (PMSN)

We assume initially for the installed PMSM application, each user carries a mobile device such as a smartphone or tablet with the same PMSN configuration what we already installed. This PMSN application is mainly developed for mobile devices by various small independent developers or group of social network providers. For our convenience only, we shall not differentiate a user from his mobile device later.

Our Proposed PMSN session totally involves two users and consists of three phases. Initially the, two users need to discover each other in the first phase like neighbor-discovery phase. Second, they need compare their individual personal profiles in the next phase called matching phase. Lastly, two matching users enter the final phase called interaction phase for real information exchange. Our work is concerned with the first and second phases.

The PMSN application uses a very fine-grained personal profiles. In particular, the application developer who develops the application defines a set of public attribute set consisting of d attributes $\{A_1, . . . ,A_d\}$, where d may range from several tens to several hundred depending on specific PMSN applications. The attributes may have different meanings in different contexts, such as interests [2], disease symptoms [7], or friends [8]. For easier illustration and identification, we hereafter assume that that each attribute corresponds to a personal interest such as movie, sports, and cooking or hobbies. To create a personal profile, every user selects an integer $u_i \in [0, \gamma -1]$ to indicate his level of area of interest in A_i (for all $i \in [1, d]$) the first time he uses the PMSN application.

B. Problem Statement: Fine-Grained Private Matching

We consider Alice with profile represented as $u = (u1, . . . , u_d)$ and Bob with profile represented as $v = (v_1, . . . , v_d)$ as two exemplary users of the same PMSN application as shown in Fig. 2. Here we assume F as a set of candidate matching metrics defined by the PMSN application developer, where each $f \in F$ is a function over two personal profiles that measure their similarity. Our private-matching protocols which are developed by application developers allow Alice and Bob to either negotiate one common metric from F or choose different metrics from F according to their own individual needs. Assume that Alice chooses a matching metric $f \in F$ and runs the privacy matching protocol with Bob to compute f(u, v). According to the amount of information disclosed during the protocol execution, we define the following three privacy levels from Alice's viewpoint, which can also be equivalently defined from Bob's viewpoint for his chosen matching metric.

C. Cryptographic Tool: Paillier Cryptosystem

Our protocols mainly rely on the Paillier cryptosystem [9], and we assume that every PMSN register user has a unique Paillier public/private key pair which can be generated via a function module of the PMSN application. How the keys are generated and used for encryption and decryption are briefed as follows to help illustrate and understand our protocols.

Key Generation:

An entity chooses two primes p and q and compute N = pq and λ = lcm (p − 1, q − 1). It then selects a random g ∈ $Z^{*}_{N^2}$ such that gcd(L(g^{λ} mod N^2),N) = 1, where L(x) = (x − 1)/N. The entity's Paillier public and private keys are (N, g) and λ, respectively.

Encryption:

Let m ∈ ZN be a plaintext to be encrypted and r ∈ Z_N be a random number. The cipher text is given by

$$E\ (m \bmod N,\ r \bmod N) = g^m r^N \bmod N^2 \qquad (1)$$

Where E (·) denotes the Paillier encryption operation using public key pk = (N, g). To simplify our expressions, we shall hereafter omit the modular notation inside E (·).

Decryption:

Given a cipher text c ∈ Z N^2 , the corresponding plaintext can be derived as

$$\mathsf{D}(c) = \frac{\mathsf{L}(c^{\lambda} \mod N^2)}{\mathsf{L}(g^{\lambda} \mod N^2)} \mod N\ , \qquad (2)$$

Where D(·) denotes the Paillier decryption operation using private key sk = λ hereafter.

The Paillier's cryptosystem has two very useful properties

Homomorphic:

For any m1, m2, r1, r2 ∈ ZN, we have E(m1, r1)E(m2, r2) = E(m1 + m2, r1r2) mod N^2, E^{m2}(m1, r1) = E(m1m2, $r^{m2}{}_{1}$) mod N^2 .

Self-blinding:

$$E(m1,\ r1)r^{N}{}_{2} \bmod N^2 = E(m1,\ r1r2)\ ,$$

Which implies that any cipher text can be changed to another without affecting the plaintext.

To facilitate our illustrations, we assume that N and g are of 1024 and 160 bits, respectively, for sufficient semantical security of the Paillier cryptosystem [10]. Under this assumption, a public key (N, g) is of 1184 bits, a cipher text is of 2048 bits, a Paillier encryption needs two 1024-bit exponentiations and one 2048-bit multiplication, and a Paillier decryption costs essentially one 2048-bit exponentiation.

4. Performance Evaluation

In this section, we evaluate the communication and computation overhead as well as overall execution time of our protocols. In our implementation, assuming that Alice initiates the matching protocol with Bob, each protocol consists of five main steps as follows.

1) Alice prepares the message through offline computation, e.g., generating a number of cipher text according to our protocol specifications.
2) Alice sends the message to indicate the start of the protocol.
3) Bob receives and buffers the message.

4) Once the transmission completes, Bob computes the intermediate result according to our protocol specifications, and sends it back to Alice.
5) On receiving the intermediate result, Alice computes the final matching result.

We use custom message headers in the application layer to distinguish these messages.

5. Conclusion

In this paper, we mainly formulated the problem of fine-grained private profile matching for proximity-based mobile social networking and presented a best suite of novel solutions that support a variety of private-matching metrics at different privacy levels. Our experimental results prove that our proposed protocols are best in private profile matching rather compared with prior work under various practical settings.

6. References

[1] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *IEEE INFOCOM '11*, Apr 2011, pp. 1–9.

[2] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in *INFOCOM'11*, Shanghai, China, Apr. 2011.

[3] "Mobile browsing by platform market share," http://marketshare.hitslink.com/mobile-phones.aspx?qprid=55&sample=31.

[4] "Facebook statistics," http://www.facebook.com/press/info.php?statistics.

[5] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in
Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), October 2007.

[6] "Global internet use reaches 1 billion," http://www.comscore.com/press/ release.asp?press=2698.

[7] M. Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "VENETA: Serverless friend-of-friend detection in mobile social networking," in *WIMOB'08*, Avignon, France, Oct. 2008.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *Mobile Networks and Applications*, pp. 1–12, 2010.

[9] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *EUROCRYPT'99*, Prague, Czech Republic, May 1999.

[10] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *INFOCOM'11*, Shanghai, China, Apr. 2011.

7. About the Authors

Konakanchi.V.S.H.Ganesh is a student of the Department of Computer Science & Engineering of Vizag Institute of Technology, Visakhapatnam. Presently he is pursuing his M.Tech from this college he received his MCA from AndhraUniversity, AP, India in the year 2011. His area of interest includes Mobile Computing- wireless communications techniques in Computer Science.

Venkata Ramana Adari is a Professor and HOD in the Department of Computer Science & Engineering of Vizag Institute of Technology, Visakhapatnam. He is having more than 20 years of experience in teaching and industry. He is a SUN CERTIFIED JAVA Professional from Sun Micro Systems, USA.His areas of interests include Software Engineering, Web mining and Object Oriented Programming. He has published several national and international research papers. He worked in Centurion University, Orissa and in some other reputed colleges in Visakhapatnam also.