IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-2, Issue-7 E-ISSN: 2347-2693

Efficient and Persistent Profile Matching in the Propinquity Mobile Social Networks

Amanullah Shaik[1*] and L N B Jyotsna[2]

[1*] *Dept. of Computer Science, Dhanekula Institute of Engg. & Technology, India*
[2]*Dept. of Computer Science, Dhanekula Institute of Engg. & Technology, India*

www.ijcaonline.org

Received: 22 /06/ 2014 Revised: 30 /06/ 2014 Accepted: 15 /07/ 2014 Published: 30 /07/ 2014

***Abstract:* -** Mobile social networks (MSNs) refer to the social networking for making new connections. In the MSNs personal preferences is an imperative service, where user can find matching users within the range. In the existing systems all services, generally all users can create specific profile and publish it into social networks to interconnect with the new people. It may contain some sensitive information also these types of sensitive users may not publish their profile into social networks as a public. A propinquity mobile social network refers to virtual interaction with the data (BLUETOOTH/WI-FI) interfaces on their smart phones. These social networks are more popular due to the recently growth of smart phone users. To reveal sensitive user's profile is most vulnerable in these devices. In these services conflicts with the user's privacy concerns about reveal their personal profiles to complete strangers before deciding to interact with them. In this paper takes this open challenge to overcome with the novel strategy. In this paper prior security work is focused on privacy to users' profiles with using high efficient symmetric cryptographic primitives.

Keywords: Privacy, Mobile Social Networking, Profile Matching, Vulnerable, Ad-Hoc Networks

I. Introduction

In traditional years Mobile Social Networks becomes more popular due to the growth of smart phone users. New generation is addicted to mobile social networks to making new connections to the new people to interact with them. In these devices users create their profile and publish for others to search easily. These social networks in smart phones enable more useful to connect virtually with their friends as face-to-face social interactions in public places such as bars, airports, trains, and stadiums [1]. In the existing systems works as, if two persons using the same application their profile is matching with some attributes then the applications are refer to both people to interact. If the any person interest to connect user can send a message to another person that person may accept or reject that inter-communication. In some cases vulnerable users may interact with the legitimate users and disclose their profiles. If users' private profiles are directly exchanged with each other, it will cause to facilitate user profiling where that information can be easily collected by a nearby user, either in an active or passive way. That user information may be exploited in unauthorized ways.

In essence, each social network offers particular services and functionalities that target a well-defined community in the real world. To make use of the provided services/functionalities and to keep being tuned with its related members, users create several accounts on various social networks. This has participated in the emergence of new users related to their needs to perform some inter network operations and services. For an example, Srihari, a software developer, is very active on social networks. He mainly uses two social networks: "face book" and "we chat" to stay connected with his friends, with the matching of users profiles.

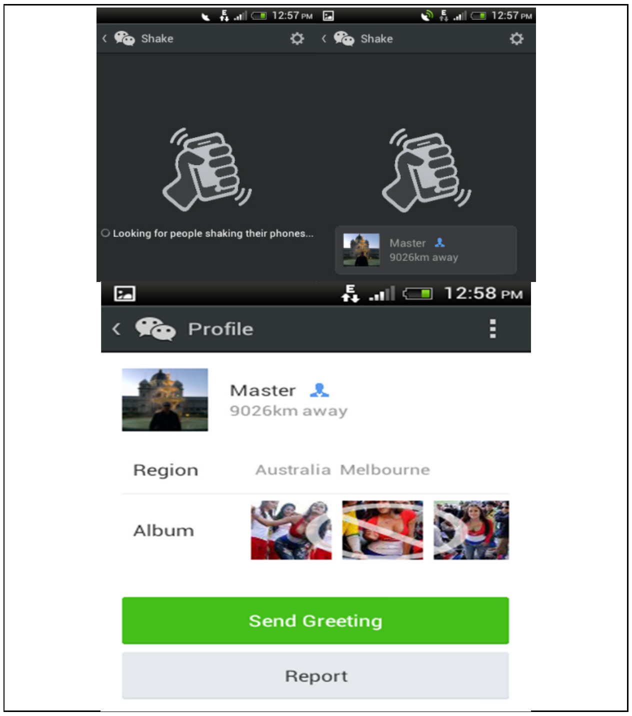

Fig: to find new people with shake their smart phones.

Corresponding Author: *Amanullah Shaik[1]*

In fact, the user profile matching consists of accurately linking users profile corresponding to user's entity. However, matching user profile on social networks is most vulnerable in the mobile devices. In some applications connect to other users with the shake their smart phones to find new friends it shows in figures.

To illustrate this, if a user wants to interconnect with the new people at anywhere just he/her shake their mobiles then it retrieves which people is using the same application with in its radar range then shown the people and gives options to "send greetings". When the user sends message to the selected user he/she may be legitimate user or vulnerable user.

For example user wants to buy a new product he/she wants to compare between the similar products and asked for a review in social networks, nearby given some suggestions either in an active way or passive way and those information may be exploited in unauthorized ways. In this way a salesmen also interact with the user then submit malicious matching queries to obtain visitor's attention for marketing purposes. To cope with user profiling in MSNs, it is essential to disclose minimal and necessary personal information to as few users as possible. To overcome these rebate mechanism in social networks we try to implement a novel strategy i.e. "FIND U". To create privacy to users' profiles used a symmetry cryptographic Multi-Party Computation (MPC) [9] mechanism.

In rest of the paper we present problem identification and introduced our approach to find social network profiles by using the set of functional properties. Finally we conclude and describe future works.

II. Problem identification

In this system consists *N* users denoted as U_1 , ….. U_n each user using smart phone. U_1 denotes as a initiator. U_1 searches the matching process and its goal is to fine best matches with it, from the rest of the users. The remaining users are called as candidates. Each user creates profile (P_i), consists set of attributes detonated as S_i, these can be strings up to a certain length. U_1 defines a matching query to a subset of S_1. It could be some variations to match the profiles. In this paper, we consider a popular similarity criterion, namely the intersection set of attributes $\{S_1 \cap S_2\}$, if the higher the similarity between two users profiles. User P_1 can first find out similarity with each other via our protocol and then will decide whether to connect with the best matching user based on their actual attributes.

Assume that mobile devices are communicating through Adhoc networks such as WI-FI/Bluetooth. Generally Adhoc network connecting devices are vulnerable on network [12]. These devices connect within the range each other. In the secure communication channel has been established between the each pair of users. We do not assume the existence of a trusted third party during the protocol run; all TTP can carry out profile matching in a completely distributed way. They may cooperate to each other.

A. Adversary model

In this paper, we primarily focused privacy to the user's profile on social networks. Here we are mainly interested and focused on social networks, insiders who are legitimate users of the matching protocol and try to perform adversary. It obtains as much personal profile information of other nearby users as possible. For example with the users attributes, a vulnerable user could correlate and identify that user via its unique id through their MAC address or public keys. However, we can't give guarantee to prevent user profiling, because at least the initiator and its best matching user will mutually learn their intersection set. For this we focus on how to minimizing and give more privacy to sensitive information revealed in one protocol run.

B. Secret handshaking

Private profile matching is also related to secret handshake/matchmaking. In secret handshake scheme [10], prove to each other the possession of some property. First, secret handshake require the communication users to have the valid credential issued by a certification authority, which will be authenticated during the handshake process, while MSN users can set and update their own personal profiles without the need to be certified by trusted third party. Moreover, support a single matching metric by requiring the perfect match between two user properties. Although the recent work [11] considers fuzzy attribute matching.

C. Design goals

Our goal is to discover the legitimate users of social profiles that refer to interact between two users. Since the users may have different privacy requirements and it takes different amount of efforts to achieve them, we informally define two levels of privacy where higher level leaks less information to the vulnerable users.

Level-0:- In the end of the protocols initiator knows mutual intersection attributes between them.

Assume that the vulnerable user has unbounded computing power, level-0 corresponds to unconditional security to all users under (Multy-party Computation) MPC. In this level vulnerable user cannot break the system by any method better than by guessing private inputs. Therefore we define level-1.

Level-1:- In the end of the protocol legitimate user knows the size of the intersection attribute set. The vulnerable user should know nothing beyond what can be derived from the above outputs and its private inputs.

Assume that, when both users will not know exactly which attributes are in the legitimate user. The vulnerable user tries to run the protocol multiple times to obtain the same amount of information with what he can obtain under level-0 when vulnerable user assumes the role of initiator.

III. Design of FIND-U

In this section, we first outline the idea of FIND-U and then present two core designs for profile sharing information protocols.

A. Overview

Here we present two protocols goal is realizing one level of privacy requirement to each. The core designs are basic design and advanced design. Realizing under level-0, this is based on secure polynomial evaluation using secret sharing. At a high level, for initiator and each user U_i , their inputs shared among a subset of U_i. The subset values remain in secret-shared forms between U_1 and U_i before their shares are revealed to each others. To reduce the communication complexity, we introduced an advancement method that aggregates multiple multiplication and addition operations into one round during the secure polynomial evaluation computation.

For advanced design achieves efficient for privacy level-1. Observe that, in the basic design if we set attribute values, then the result will be 0, otherwise a random number, in order to obtain the number of matching profiles, one way is to employ the equality test protocol [2]. However this method incurs too high communication cost, since even the most efficient algorithm takes 12k invocations of the multiplication protocol.

Thus, we adopt a blind-and-permute method to obliviously permute initiator shares of each attribute, so that the linkage between application and its corresponding attribute is broken. This method between two users U_1 and U_2 where each data item is additively split between them is described in [3]. Our goal is, U_1 encrypts each of its shares using additive homomorphism encryption and sends to each U_2. U_2 then generates a different random number for each shared item, and randomizes each U_1 shares using a pseudo-random permutation, and sends back to initiator. All the computations are done over the cipher texts. However, blind-and-permute can't be applied directly. In our protocol each user is polynomial shared with another user.

B. Privacy levels

User can choose he/her privacy level by telling other users he/her choice in the initiator. For example initiator wants to sends a broadcast messages it indicating to level-o privacy. Then the other users computing attributes and reconstruction sets will follow the basic design. However, the initiator should always agree on the privacy level that each candidate proposes, since U_1 is at a position to conduct user profiling.

We can foresee that FIND-U mechanism is used in the mobile devices equipped with short-range wireless interfaces, and operate in the Adhoc mode. We have done some prior work on practical trust initialization in Adhoc networks [4]. In this possible setup process that involve human effort.

C. User finding

If using Bluetooth, the existing service discovery protocol (SDP) can be utilized to search for nearby users within the range. SDP [5] protocol can be used to publish information. We can use it to initiate the protocol (key establishment). For WI-FI, the Adhoc mode would be sufficient for device discovery.

For giving privacy we can uses symmetric cryptographic values. In the cryptographic it uses the key establishment, as pair wise keys should be established between all nearby users, a straightforward design like Bluetooth devices manually pair up with all the users would require $O(N^2)$ complexity. In order to complex and minimize the need of explicit human participation, Diffie-Hellman key exchange (DHKE) can be used. This approach is more favorable for WI-FI devices with richer resources however, for Bluetooth devices it can also be used. We note that although the SDP protocol does not support broadcast, each device can establish up to 10 numbers with a maximum of 128 bytes each [5]. This would be sufficient DHKE with 1024- bit group size.

IV. Security

In this paper we used security for giving privacy to user’s profile, Multi-Party-Computation (MPC). Assume that private channels. Loosely speaking, “a multi-Party protocol privately computes attributes. If whatever a set of legitimate users can obtain after participating in the protocol could be essentially obtained from the input and output of these users”, this protocol compute two-ary functionality between the initiator U_1 and other user U_2, $F(U_1,U_2)=U_1\cap U_2$ i.e., $p\backslash\{U_1,U_2\}$ do not have inputs nor any output. It follows the real-world paradigm.

A. Preventing vulnerable attacks

In our protocol a specific type of “set inflation attack” can be easily prevented where vulnerable user influences the final output in he/her favorable way by changing, shares after seeing others’.

Further, we observe it is possible that our protocol can be extended to the malicious model with some additional cost following the same method [6]. The idea is to use verifiable secret sharing (VSS) [7],[8]. This is secure under the vulnerable users. Asharov and Lindell proved in [6], with a VSS scheme and a secure multiplication protocol functional attributes that is based on VSS. However this protocol is expensive in communication, and does not protect against active attacks.

V. Conclusion

In this paper, first formalize the problem of privacy in users profile in mobile social networks, and propose two privacy level protocols that achieve increasing levels of user privacy presentation. Our schemes are much more efficient that state-of-the-art ones in MSNs where the network size is the order of tens, and when the number of query attributes is smaller than number of profile attributes. However this protocol is expensive in communication, and does not protect against active attacks. As a future work, we are planning to further explore and propose more interesting inter-social operations and functionalities.

Acknowledgement

Most of all, I shall give all glory, honor and thank to my parents. They made me as I am. Then there are a few people I would like to thank, my guide Mrs. L N B Jyostna madam, who spared no effort to ensure that I have everything I needed. Finally my friends who gave their time, love and energy.

References

[1]. Z. Yang, B. Zhang, J.Dai, A.Champion, D.Xuan, and D. Li, “E-smart Talker: A distributed mobile system for social networking in physical proximity,” in ICDCS’10, Genoa, Italy, June 2010, pp. 468-477.

[2]. T. Nishide and K. Ohta, “Multyparty Computation for interval, equality, and comparisons without bit-decomposition protocol,” in PKC’07,2007, pp. 343-360.

[3]. Y. Qi and M. J. Atallah, “Efficient privacy-preserving K-nearest neighbor search,” in IEEE ICDCS’08,2008, pp. 311-319.

[4]. M. Li, S. Yu, J.D. Guttman, W. Lou, and K. Ren, “Secure Adhoc trust initialization and key management in wireless body area networks,” ACM Transactions on sensor Networks(TOSN), 2012.

[5]. Z. Yang, B. Zhang, J. Dai, A. Champion, D. Xuan, D. Li, “E-smarttaliker: A distributed mobile system for social networking in physical proximity,” in IEEE ICDCS’10, June, 2010.

[6]. G. Asharov and Y. Lindell, “ A full proof of the bgw protocol for perfectly-secure multiparty computation,” Advances in CryptologyCRYPTO 2011,2011.

[7]. M. Ben-Or, S.Goldwasser, and A.Wigderson,”Completeness theorems for non-cryptographic fault-tolerant distributed computation.”

[8]. R. Gennaro, M.O.Rabin, and T. Rabin, “simplified vss and fast-track multiparty computations with applications to threshold cryptography,” in ACM PODC ’98, 1998, pp. 101-111.

[9]. Josef Pieprzyk , Hossein Ghodosi and Ron Steinfeld, “multi-Party Computation with Conversion of secret Sharing,” NTU, Singapore, September 2011.

[10]. R. W. Baldwin and W. C. Gramlich, “Cryptographic protocol for trustable match making,” in IEEE S&P’85, Oakland, CA,April 1985.

[11]. G. Ateniese, M. Blanton, and J. Kirsch, “Secret handshakes with dynamic and fuzzy matching,” in NDSS’07, San Diego, CA, FEB. 2007.

[12]. Srihari babu. Kolla and B B K Prasad, “A Survey of Source Routing Protocols, Vulnerabilities and Security in wireless Adhoc networks” IJCSE vol 2 no.4 pp. 20-25. April 2014.

Authors’ profile

Amanullah. Shaik is perusing Masters’ degree in computer science and engineering, JNTU KAKINADA. His research interested in network security, privacy and anonymity, low-power networks, security for sensor networks and mobile applications.

Mrs. L N B Jyostna is assistant professor in Department of computer science & engineering in Dhanekula institute of engineering and technology at Vijayawada in India. She has 6 years’ experience in teaching. She is interested in the field of modern communication systems and developments in wireless technology.