International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Fully Anonymous Privacy Protection Profile Matching in Mobile Social Networks

Dr.K.Venkateswara Reddy[1]; K.L.Narasimha Rao[2]& P.Sravanthi[3]

[1]Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

[2]Associate Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

[3]M.Tech CS (PG Scholar),Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

ABSTRACT

Privacy-preservation in movable community set of connections (msns) and begin a family of novel summary identical protocols. We first propose a clear Comparison-based summary identical protocol which runs between two parties, an originator and a responder. The summary identical protocol enables the originator to get hold of the comparison-based matching result about a specified attribute in their profiles, while avoid their characteristic values from disclosure. Then we propose an implicit Comparison-based Profile matching protocol which allows the originator to straight get hold of a number of messages instead of the comparison result from the responder. The messages not linked to user profile can be separated into many groups by the responder. The originator completely decides the interested group which is unidentified to the responder. Two messages in both groups are prepared by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute. We further generalize the icpm to an implicit Predicate-based Profile matching protocol which allows complex comparison criteria spanning multiple attributes. The anonymity analysis shows all these protocols achieve the confidentiality of user profiles. In addition, the eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM do not reveal the result at all and provide full anonymity. We analyze the communication overhead and the anonymity strength of the protocols. We then present an enhanced version of the eCPM, called eCPM+, by combining the eCPM with a novel prediction-based adaptive pseudonym change strategy. The performance of the eCPM and the eCPM+ are comparatively studied through extensive trace-based simulations. Simulation results demonstrate that the eCPM+ achieves significantly higher anonymity strength with slightly larger number of pseudonyms than the eCPM.

Keywords: Mobile Social Network; Profile Matching; Privacy Preservation

I. INTRODUCTION

Social networking makes digital communication technologies sharpening tools for extending the social circle of people. It has already become an important integral part of our daily lives, enabling us to contact our friends and families on time. As reported by ComScore, social networking sites such as Facebook and Twitter have reached 82 percent of the world's online population,

representing 1.2 billion users around the world. In the meantime, fuelled by the pervasive adoption of advanced handheld devices and the ubiquitous connections of Bluetooth/WiFi/GSM/LTE networks, the use of Mobile Social Networking (MSNs) has surged [1]. In the MSNs, users are able to not only surf the Internet but also communicate with peers in close vicinity using short-range wireless communications.

The social networking sites like Face book and Twitter have reached 82 percent of the world's online population, representing 1.2 billion users around the world. Meanwhile, driven by the widespread adoption of advanced hand devices and ubiquitous network connections Bluetooth / Wi-Fi / GSM /LTE, the use of mobile social networking (MSN) has exploded [2]. In MSN, users are able to not only surf the Internet, but also communicate with their peers in the vicinity that use the short-range wireless communications. Due to its geographical nature, the MSN support many promising and innovative applications for example, through the Bluetooth communications, People Net allows searching for effective information between mobile phones neighbors; a message-relay approach is suggested in to facilitate ride sharing and ride sharing in a local region. Realizing the potential benefits presented by MSN, recent research efforts have been made on how to improve the effectiveness and efficiency of communications among users of MSN [3]. They developed specialized routing protocols and data forwarding associated with the social characteristics exhibited by the behavior of users, such as social friendship, social selfishness and social morality. It is encouraging that traditional solutions can be expanded further to troubleshoot MSN, considering the unique social characteristics.

Privacy preservation is an important research topic in social networks. Given that more personal information is shared with the public, violating the privacy of a target user is much easier. Research efforts have been put into the presentation of identity and privacy issues on social networking sites. Gross and Acquisti argued that users are jeopardizing both offline [4] (eg, stalking) and online (eg, identity theft) based on an analysis of the behavior of more than 4,000 students they have joined a popular social network presented a quantitative analysis of identity information disclosure in social network communities and the subjective opinions of students regarding the identity protection and information disclosure. When social networking platforms extend into the mobile environment, users require more extensive privacy preservation because they are unfamiliar with neighbors nearby that can spy, store and correlate their personal data in different periods and places [5]. Once personal information is correlated with the location information, the user behavior will be fully disclosed to the public. Chen and Rahman studied various mobile social networking applications (SNAS), such as neighborhood exploring applications for mobile and SNAs specific content sharing applications, which do not provide feedback or control mechanisms for users and can cause localization inappropriate and identity information disclosure [6].

Privacy preservation is a significant research issue in social networking. Since more personalized information is shared with the public, violating the privacy of a target user become much easier. Research efforts have been put on identity presentation and privacy concerns in social networking sites. Gross and Acquits argued that users are putting themselves at risk

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

both offline (e.g., stalking) and online (e.g., identity theft) based on a behavior analysis of more than 4,000 students who have joined a popular social networking site. Stutsman presented a quantitative analysis of identity information disclosure in social network communities and subjective opinions from students regarding identity protection and information disclosure. When the social networking platforms are extended into the mobile environment, users require more extensive privacy-preservation because they are unfamiliar with the neighbors in close vicinity who may eavesdrop, store, and correlate their personal information at different time periods and locations. Once the personal information is correlated to the location information, the behavior of users will be completely disclosed to the public.

II. EXISTING SYSTEM

Mobile social networks as emerging social communication platforms have attracted great attention recently, and their mobile applications have been developed and implemented pervasively. 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. introduced a distributed mobile communication system, called E-Small Talker, which facilitates social networking in physical proximity. ESmallTalker automatically discovers and suggests common topics between users for easy conversation. Lu et al. 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 [7].

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, 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. implemented profile matching with more operations including set intersection, union, cardinality and over-threshold operations. On the other hand, Ye et al. further extended the FNP scheme to a distributed private matching scheme and Dachman-Soled et al. aimed at reducing the protocol complexity. All the above solutions to the set intersection rely on homomorphic encryption operation [8].

In the meantime, other works employed an oblivious pseudo random function to build their profile matching protocols, where communication and computational efficiency is improved. Li et al. implemented profile matching according to three increasing privacy levels [9]:

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 [10]. The icpm and the ippm do not reveal the result at all and provide full anonymity. Users require more extensive privacy-preservation because they are

unfamiliar with the neighbors in close vicinity who may eavesdrop, store, and correlate their personal information at different time periods and locations. The improved protocol only reveals whether the dot product is above or below a given threshold. The threshold value is selected by the user who initiates the profile matching [12]. They pointed out the potential anonymity risk of their protocols. The threshold value must be larger than a pre-defined lower bound (a system parameter) to guarantee user anonymity. The homomorphic encryption schemes that support different operations such as addition and multiplication on cipher texts. The user is able to process the encrypted plaintext without knowing the secret keys [13].

The dot product protocol is lack of verifiable secure computation. The Protocol only reveals whether the dot product is above or below a given threshold. They pointed out the potential anonymity risk of their protocols; an adversary may adaptively adjust the threshold value to quickly narrow down the value range of the victim profile. It Present an enhanced version of the ecpm, called ecpm+, by combining the ecpm with a novel prediction-based adaptive pseudonym change strategy. The performance of the ecpm and the ecpm+ are comparatively studied through extensive trace-based simulations. The ecpm+ achieves significantly higher anonymity strength with slightly larger number of pseudonyms than the ecpm. The msns, users are able to not only surf the Internet but also communicate with peers in close vicinity using short-range wireless communications [14, 15]. The social features exhibited from the behavior of users, such as, social friendship social selfishness and social morality. It is encouraging that the traditional solutions can be further extended to solve the MSN problems by considering the unique social features [16].

The homomorphic encryption schemes are widely used in data aggregation and computation specifically for privacy-sensitive information. We review the homomorphic encryption scheme that serves a building block of our proposed profile matching protocols. The profile matching protocols are novel since the comparison of attribute values is considered as the matching operation [17].

Threats in Mobile Social Networks:

1. Digital record aggregation: Profiles on MSNs can be downloaded and stored by third parties, creating a digital record of private data.

2. Secondary data collection: Information knowingly revealed in a profile. Various researches propose that such data is being used to significant monetary gain.

3. Face recognition: User-provided digital images are a very popular part of profiles on MSNs. The picture is, in effect, a binary identifier for the user, allowing linking across profiles.

4. Difficulty of complete account deletion: Users aspiring to remove accounts from MSNs discover that it is more or less not possible to delete secondary information linked to their profile such as public comments on other profiles.

5. Difficult to guard from malicious users who are snooping about the personal information of other users.

6. Difficult to safeguard from neighbors in mobile environment who may snoop, store, and compare their personal information.

7. The Internet stores an everlasting record of the conversation which can be tracked.

8. Using non-secure passwords might perhaps be without difficulty guessed by cyber criminals and compromise your MSN account to spam your contacts [18].

III. PROPOSED SYSTEM

We first propose an explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, an initiator and a responder. The eCPM enables the initiator to obtain the comparison-based matching result about a specified attribute in their profiles, while preventing their attribute values from Disclosure. We then propose an implicit Comparison-based Profile Matching protocol (iCPM) 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. We further generalize the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes. The anonymity analysis shows all these protocols achieve the confidentiality of user profiles. In addition, the eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM do not reveal the result at all and provide full anonymity. We analyze the communication overhead and the anonymity strength of the protocols.

We first worked on an explicit Comparison-based Profile matching protocol (eCPM) which happens among two users, an initiator and a responder. The eCPM allows the initiator to attain the comparison-based matching outcome regarding a particular attribute in their profiles, at the same time as stopping their attribute values from revelation.

Later on we examined an implicit Comparison-based Profile matching protocol (iCPM) which permits the initiator to straight forwardly get various messages as an alternative of the evaluation outcome from the responder. The messages unrelated to user profile can be divided into multiple categories by the responder. The initiator totally prefers the concerned category which is unfamiliar to the responder. Two messages in every category are arranged by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute.

We additionally generalized the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which facilitates multifaceted evaluation criteria across several attributes. The anonymity investigation demonstrates that all these protocols accomplish the confidentiality of user profiles. Apart from the above, the eCPM reveals the evaluation outcome to the initiator and provides simply conditional anonymity; the iCPM and the iPPM do not disclose the outcome at all and give full secrecy.

Merits of the proposed system:

1) Two commonly unknown users, both holding confidential information, together calculate the possible correlation without revealing any extra data to other user.

2) Make possible open communication, leading to improved information detection and delivery.
3) Permits users to talk about thoughts, ask questions and share links.

IV. Conclusion

An exceptional comparison-based profile matching difficulty in Mobile Social Networks (MSNs) has been addressed, and new methods are projected to resolve it. The explicit Comparison depending on Profile Matching (eCPM) protocol provides conditional secrecy. It discloses the evaluation outcome to the initiator. Taking into account the k-anonymity as a user condition; the anonymity risk level in relation to the pseudonym change for successive eCPM runs is studied and observed. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) has been simulated and worked upon. The iCPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression consists of multiple comparisons across several attributes. The iCPM and the iPPM both allow users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile data.

REFERENCES

[1]. Raad, E. ; LE2I, Bourgogne Univ., Dijon, France ; Chbeir, R. ; Dipanda, A.,User Profile Matching in Social Networks, 13th International Conference on Network-Based Information Systems (NBiS), 2010.

[2]. Rui Zhang, Jinxue Zhang, Yanchao Zhang, Jinyuan Sun, and Guanhua Yan, Privacy-preserving profile matching for proximity based mobile social networking, IEEE Journal on Selected Areas in Communications,Special Issue on Emerging Technologies in Communications, 2012.

[3]. Wei Dong ; Univ. of Texas at Austin, Austin, TX, USA ; Dave, V. ; LiliQiu ; Yin Zhang,Secure friend discovery in mobile social networks,INFOCOM, 2011 Proceedings IEEE.

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

[5] 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.

[6] M. Motani, V. Srinivasan, and P. Nuggehalli, "People net: engineering a wireless virtual social network," in MobiCom, 2005, pp. 243–257.

[7] 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.

[8] 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.

[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 ICDCS, 2010, pp. 468–477.

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

[11] 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.

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

[13] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Moralitydriven data forwarding with privacy preservation in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 7, no. 61, pp. 3209–3222, 2012.

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

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

[16] 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.

[17] 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.

[18] 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.