INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

COMPLETELY UNIDENTIFIED PROFILE MATCHING IN MOBILE SOCIAL NETWORKS

[1]Akkanagamma, [2]C.H.Kiran

[1]Department of Computer Science and Engineering, TIST, JNTUH. TS. INDIA.
[2]Department of Computer Science and Engineering, TIST, JNTUH. TS. INDIA.
[1]akku.nara2807@gmail.com, [2]kiran.30.aug@gmail.com.

Abstract

In user profile matching with privacy-preservation in mobile social networks (MSNs) introducing a number of novel profile matching protocols. First we proposing an explicit Comparison-based Profile Matching protocol (eCPM) which runs between an initiator and a responder. The eCPM enables the initiator to obtain the comparison-based matching result about a specific attribute in their profiles, while preventing those attribute values from disclosure. Next we 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 which are unrelated to user profile can be divided into multiple categories by the responder. Then initiator implicitly chooses the interested category which is unknown for the responder. Two messages of each category are prepared by the responder, and only one message can be accepted by the initiator based on the comparison result on a single attribute. Then 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 above protocols achieve the confidentiality of user profiles. The eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM will not reveal the result to initiator and provide full anonymity. By these protocols analyze the communication overhead and the anonymity strength of the protocols. Next we presenting an enhanced version of eCPM, called eCPM+, by combining the eCPM with prediction-based adaptive pseudonym change strategy. This performance of the eCPM and the eCPM+ are comparatively studied through extensive trace-based simulations. Simulation of results demonstrates that, the eCPM+ achieves significantly higher anonymity strength with slightly larger number of pseudonyms than the eCPM.

1. Introduction

Social networking makes digital communication technologies sharpening tools for extending the social network of people. It has already become an important integral part of our daily life, facilitating us to contact our friends and families. As stated by ComScore, social networking sites such as Facebook and Twitter have reached 82% of the world's online population, representing around 1.2 billion users in the world. Meanwhile, fueled by the pervasive adoption of advanced handheld devices and the ubiquitous connections such as Bluetooth/WiFi/GSM/LTE networks, the use of Mobile Social Networking (MSNs) has surged. In the MSNs, users are able to not only access the Internet but also communicate with other peers in close vicinity using short-range wireless communications.

Due to geographical nature of MSN, the MSNs support many promising and innovative applications. For example, through Bluetooth communications, People Net enables effectual information search among neighbors self phones; a message-relay approach is suggested that to facilitate carpool and ride the sharing in a local region. Realizing the potential benefits of the MSNs, recent research efforts have been concentrating on how to improve the effectiveness and efficiency of the communications among the MSN users. Then they developed specialized data routing and forwarding protocols which are associated with the social features exhibited from the behavior of users, such as, social selfishness, social friendship, and social morality. It was encouraged that the traditional solutions can be further more extended to solve the problems of MSNs by considering the unique social networking features.

Privacy preservation is the best significant research issue in social networking in MSNs. Since more and more personalized information of the users is shared with to public, violating the privacy of a targeted user become much easier. Research efforts put on identity presentation and privacy concerns of social networking sites. Gross and Acquisti reported that users are putting themselves at risk both offline (e.g., stalking) and online (e.g., identity theft) according o the behavior analysis of more than 4,000 students who had joined a popular social networking site. Stutz man 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 to the mobile environment, for that users require more extensive privacy-preservation because they are not familiar with the neighbors in close to them, who may store, eavesdrop and correlate their personal information at particular locations and different time periods. If the personal information is correlated to the location information, at that time behavior of users will be completely disclosed as publically. Chen and Rahman reported various mobile Social Networking Applications (SNAs), such as, mobile-specific SNAs, neighborhood exploring applications, and content-sharing applications, which provide no feedback or control mechanisms to users and cause inappropriate location and identity information disclosure to initiator. To overcome this privacy violation in MSNs, so many privacy enhancing techniques had been adopted into the MSN applications. For example, when two users approach in the MSNs, privacy-preserving profile matching acts as a critical mandatory initial step to help users, especially to strangers, initializes conversation with one another in a distributed and privacy-preserving manner. Many researches on the privacy preserving profile matching have been carried out and the common goal of these works is to enable the handshake between two approached users if both users satisfy with each other's requirement while hiding the unnecessary information from the disclosure if they are not. The original idea is an agent of the Central Intelligence Agency (CIA), wants to authenticate itself to a server, but will not reveal it's CIA credentials unless the server is a genuine CIA outlet. Meanwhile, the server will not reveal its CIA credentials to anyone than CIA agents.

2. Existing System

Privacy preservation is a most significant research issue in mobile social networking. The social networking platforms are extended into the mobile environment, where users require more extensive and effective privacy-preservation because they are not familiar with the neighbors in close to them, who may store, eavesdrop and correlate their personal information at particular locations and different time periods. If the personal information is correlated to the location information, at that time behavior of users will be completely disclosed as publically. Chen and Rahman reported various mobile Social Networking Applications (SNAs), such as, mobile-specific SNAs, neighborhood exploring applications, and content-sharing applications, which provide no feedback or control mechanisms to users and cause inappropriate location and identity information disclosure to initiator. To overcome this privacy violation in MSNs, so many privacy enhancing techniques had been adopted into the MSN applications.

3. Proposed system

We firstly proposing an explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, such as an initiator and a responder. Initially eCPM enables the initiator to obtain the comparison-based matching result about a specific attributes in their profiles, while preventing those attribute values from disclosure. Next we 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 which are unrelated to user profile can be divided into multiple categories by the responder. Then initiator implicitly chooses

the interested category which is unknown for the responder. Two messages of each category are prepared by the responder, and only one message can be accepted by the initiator based on the comparison result on a single attribute. Then 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 above protocols achieve the confidentiality of user profiles. The eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM will not reveal the result to initiator and provide full anonymity.

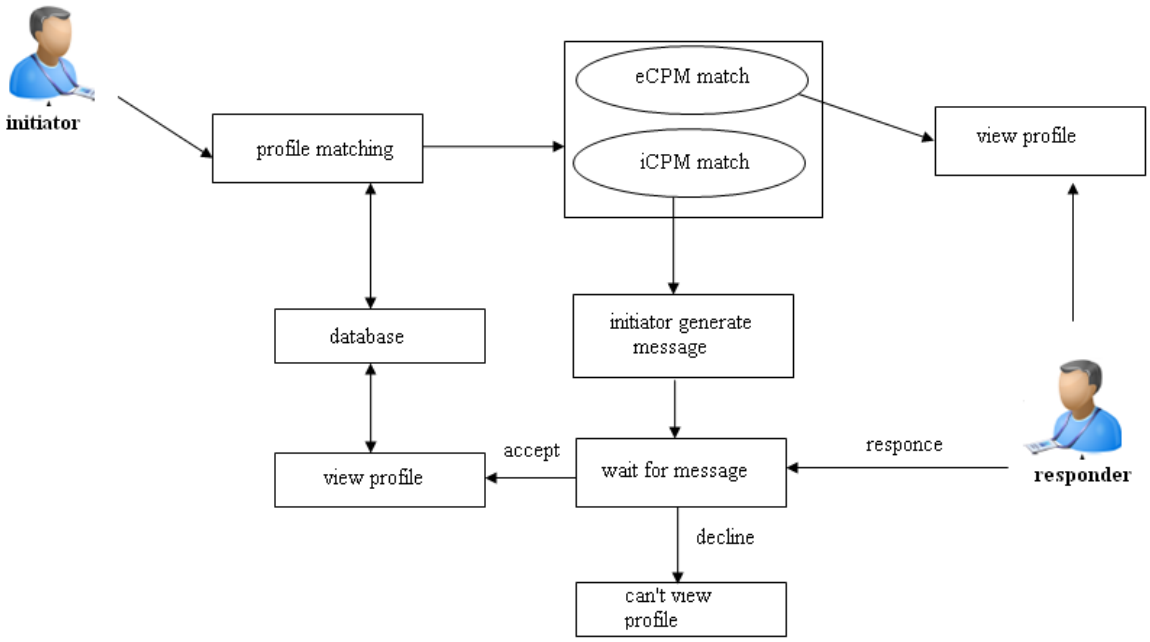

Fig: Interaction between initiator and responder

4. Literature survey

Literature survey is the one of the important stage in software development process. Before we developing the tool it is necessary to determine the time factor and economy. Once these things are satisfied, then next steps are to determine using which operating system and language the tool can be developed. Once the programmers has started building the tool, then programmers requires lot of external support. This support can be obtained from senior programmers, from websites or from books. Before building the tool above considerations are taken into account for developing the proposed system.

5. Profile Matching Protocols

5.1 Explicit Comparison-based Profile Matching (eCPM) Module:

Attribute, the eCPM allows the initiator to know the comparison result, i.e., whether it has a larger, equal, or smaller value than the responder on the attribute. Due to the exposure of the comparison result, user profile will be leaked and linked in some conditions. We provide a numerical analysis on the conditional anonymity of the eCPM. We study the anonymity risk level in relation to the pseudonym change for the consecutive eCPM runs.

5.2 Implicit Comparison-based Profile Matching (iCPM) Module:

We propose the iCPM, in this protocol; the responder prepares multiple categories of messages where two messages are generated for each category. The initiator can obtain only one message related to one category for each run. During the protocol, the responder is unable to know the category of the initiator's interest. To receive which message in the category is dependent on the comparison result on a specified attribute. The responder does not know which message the initiator receives, while the initiator cannot derive the comparison result from the received message. We provide an analysis of the effectiveness of the iCPM, and show that the iCPM achieves full anonymity.

5.3 Privacy Preserving Module:

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. 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.

6. Data-flow Diagrams

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

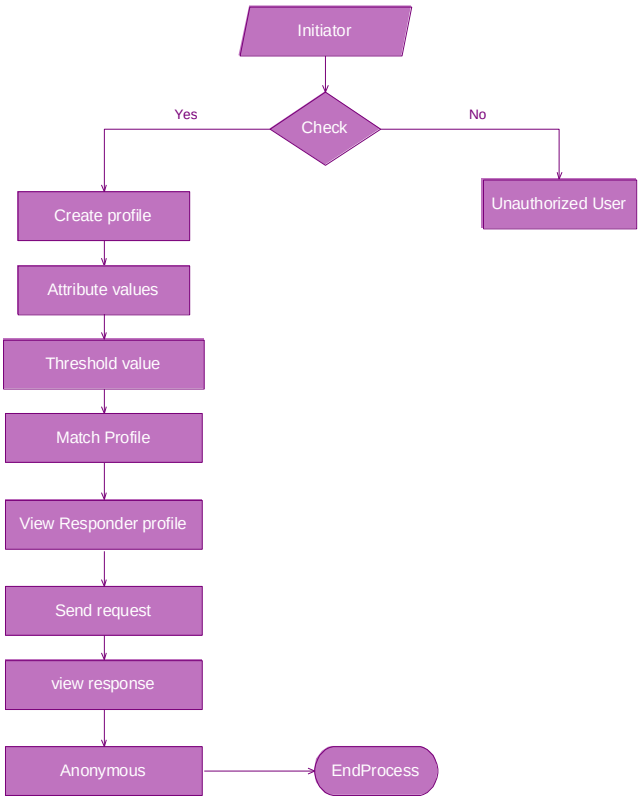

Fig: Data-Flow diagram for initiator

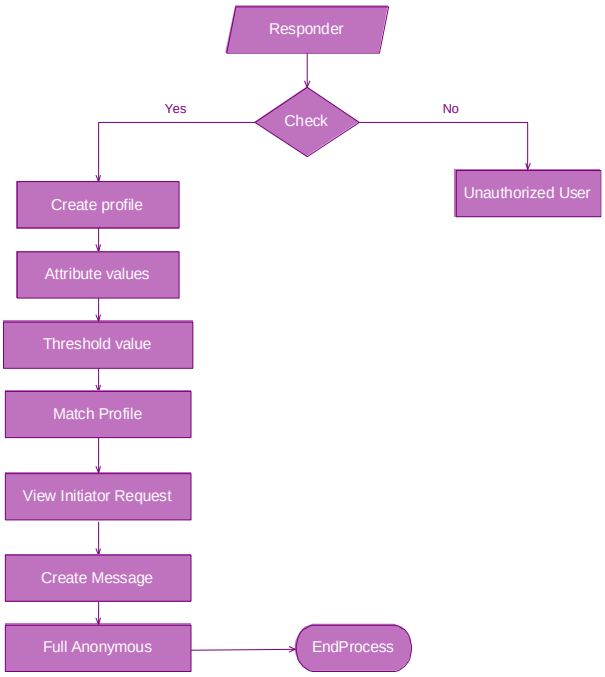

Fig: Data-Flow Diagram for Responder

7. Conclusion

We have investigated a unique comparison-based profile matching problem in Mobile Social Networks (MSNs), and proposed novel protocols to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional anonymity. It reveals the comparison result to the initiator. Consider the *k*-anonymity as a user requirement; we analyze the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs. We have also devised two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM). 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, we implement “>” and “<” operations for profile matching. One future work is to extend them to support more operations, such as “≥” and “≤”. Another future work is to hide the predicate information in the iPPM. Currently, the responder needs to transmit the threshold value of the predicate to the initiator, which may reveal partial information of the responder’s interest. Restricting the disclosure of such parameter will be of significance for advancing comparison-based family of profile matching protocols and warrants deep investigation.

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 adhoc- 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.

Sites Referred:

http://java.sun.com
http://www.roseindia.com/
http://www.java2s.com/