Research Paper

Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

Friending in Mobile Social Networks: Current Trends and Research Challenges

Engineering

KEYWORDS : Mobile Social Networks, Privacy Preserving, Friending

Ms. Ruchika D. Ganvir — Dept. of Computer Engineering SSGMCE, Shegaon

Prof. Vishwanath Mahalle — Dept. of Computer Engineering SSGMCE, Shegaon

ABSTRACT

The rise of mobile social networks is inextricably linked with the revolution in mobile computing, which has spawned a huge industry in mobile application development. Localization techniques such as GPS, has made it possible to share the location information on mobile social networks. Positioning technologies such as Wireless localization techniques, and Global Positioning System gives rise to location-aware social networks. But the location data posted to social networks are revealing sources, too. Hence Friending has become the challenging part of Mobile social networks.

This paper discusses the recent trends of friending in mobile social networks and briefly peeks into the research challenges.

Introduction

Friending and communication are two important basic functions of social networks. When people join social networks, they usually begin by creating a profile, then interact with other users. The content of profile could be very broad, such as personal background, hobbies, contacts, places they have been to. Profile matching is the key component of mobile social networking apps, since it is a common and helpful way to make new friends with common interest or experience, find lost connections, or search for experts. Some applications help a user automatically find users with similar profile within a certain distance. MagnetU [1] matches one with nearby people for dating, friend-making. Small-talks [2] connect proximate users based on common interests. These applications use profiles to facilitate friending between strangers and also enable privacy preserving people searching to some extent. Observe that in practice the mobile Internet connection may not always be available and it may incur high expense. Thus, the availability of short-range wireless technology such as WiFi and Bluetooth makes it possible to build a new class of proximity-based decentralized (or ad hoc) social networks with mobile phones [3].

However the increasing privacy concern becomes a barrier for mobile ad hoc social networking. People are unwilling to disclose personal profiles to arbitrary persons in physical proximity before deciding to interact with them. The insecure wireless communication channel and potentially malicious service provider increase the risk of revealing private information.

Current situation of friending in Mobile Social Networks

Most previous private matching work is based on the secure multi-party computation (SMC) [4]. There are two mainstreams of approaches to solve the private profile-based friending problem. The first category is based on private set intersection (PSI) and private cardinality of set intersection (PCSI). Early work in this category mainly addresses the private set operation problem in database research, *e.g.* [5], [6], [7], [8]. Work like [9] studied the problem of private k nearest neighbor search. Later on some work treat a user's profile as multiple attributes chosen from a public set of attributes and provide well-designed protocols to privately match users' profiles based on PSI and PCSI, [10], [11]. The second category is based on private vector dot product [12]. [13] considers a user's profile as vector which represents his/her social coordinate, and the social proximity between two uses as the matching metric. It calculates the metric by private dot product. A trusted central server is required to precompute users social coordinates and generate certifications and keys. [14] improves these work with a fine-grained private matching by associating a user-specific numerical value with every attribute to indicate the level of interest. However, most these approaches lack a specific definition of matching user. For example, in the PSI based schemes, any user can learn the profile intersection with any other user despite the similarity between them. The PCSI and dot product based approaches cannot support a precise specific profile matchings.

These protocols often rely on public-key cryptosystem and/or homomorphic encryption, which results in expensive computation cost and usually requires a trusted third party. Even non-matching users involve in the expensive computation. Multiple rounds of interactions are required to perform the private profile matching between each pair of parties. They all need preset procedure, *e.g.* exchanging public keys before matching, precomputing vector [13], establishing secure communication channel and share secret [10]. Furthermore, these protocols are unverifiable.

Mobile Social Networks -Research Challenges

The following will discuss security and privacy problems associated with peer-to-peer and client-server mobile social network systems. Since there are differences between the peer to-peer and client-server architectures, we will indicate which issues apply to a particular architecture.

Direct Anonymity Issues

The information exchange model of the mobile social network systems discussed previously provide little protection for the user's privacy. These systems require the user to allow access to his or her social network profile information and at the same time associate that information with the user's identity. For instance, Facebook applications generally require the user to agree to give the application access to his/her information through Facebook's API, intrinsically tying such information to the user's identity. In the WhozThat and SocialAware systems, anyone near the mobile user can use a Bluetooth device to snoop a user's shared social network ID or eavesdrop on data sent openly over a wireless connection, since all data transmitted over the wireless connection is sent in the clear, although relatively weak provisions for link-layer encryption exist [15].

In a peer-to-peer context-aware mobile social network system such as SocialAware, we can track a user by logging the date and time that each mobile or stationary device detects the user's social network ID. By collecting such logs, we can construct a history of the locations that a user has visited and the times of each visit, compromising the user's privacy. Finally, given access to a user's social network ID, someone else could access that user's public information in a way that the user may not have intended by simply viewing that user's public profile on a social network Web site. We conclude that cleartext exchange of social networking IDs in systems such as WhozThat and SocialAware

leads to unacceptable security and privacy risks, and allows the user's anonymity to be easily compromised. We call such problems that directly compromise a user's anonymity *direct anonymity attacks*.

The Indirect or K-Anonymity Problem

One worthwhile challenge is that of supporting complex mobile social networking applications with personal information without compromising the anonymity of the users providing the information. Even if the user does not directly provide his/her identification information, the user's provided social network information (such as preferences) may be mapped back to the user's identity through the social network site or information cached within mobile and stationary devices in the environment. The indirect anonymity problem exists when a piece of information indirectly compromises a user's identity. An example of this is when a piece of information unique to a user is given out, such as a list of the user's favorite movies, this information might then be easily mapped back to the user. The *K*-anonymity problem occurs when *n* pieces of information or *n* sets of related information can be used together to uniquely map back to a user's identity. Furthermore, if a set of information can only be mapped to a set of *k* or fewer sets of users, the user's anonymity is still compromised to a degree related to *k*. The challenge is to design an algorithm that can decide what information should and should not be given out in order to guarantee the anonymity of associated users. The abundance and diversity of social network information makes this privacy guarantee more complicated than it may initially appear. More formally, the particular problem is to find what personal information can be shared such that this information cannot be used to associate the user's identity with a specific context.

Eavesdropping, Spoofing, Replay, and Wormhole Attacks

Once a user's social network ID has been intercepted in a peer-to-peer mobile social network system, it can be used to mount a replay and spoofing attack. In a spoofing attack, a malicious user can masquerade as the user whose ID was intercepted (the compromised user) by simply sending (replaying) the intercepted ID to mobile or stationary devices that request the user's social network ID. Thus, the replay attack, where the compromised user's ID is maliciously repeated, is used to perform the spoofing attack. Another specific type of replay attack is known as a wormhole attack [16], where wireless transmissions are captured on one end of the network and replayed on another end of the network. In a system such as WhozThat or SocialAware, a malicious user could use a wormhole attack to capture a user's ID and masquerade as that user in a different, perhaps distant, location. Since these systems are vulnerable to such replay and spoofing attacks, we can no longer trust that each user who participates in these systems is really who they claim to be. Clearly, spoofing attacks in mobile social networking systems present serious security risks.

In addition to intercepting a user's social network ID via eavesdropping of the wireless network, a malicious user could eavesdrop on information transmitted when a device requests a user's social network profile information from a social network server.

Eavesdropping, spoofing, replay, and wormhole attacks are generally not major threats to client-server mobile social network systems. These attacks can be defended against with the appropriate use of a robust security protocol such as HTTPS, in conjunction with client authentication using user names and passwords or client certificates.

Conclusion

This paper examined mobile social networks as a new multidisciplinary research field that bridges social science and multimedia computing. It introduced the most important aspects of social networks by considering two main aspects: trends and challenges. The goal of this publication was to provide an initial base line to build a discussion forum on the most critical issues related to mobile social networks.

REFERENCE

[1] Magnetu. http://magnetu.com. | [2] Yang, Z., Zhang, B., Dai, J., Champion, A., Xuan, D., and Li, D. E-smalltalker: A distributed mobile system for social networking in physical proximity. In Proc. IEEE ICDCS, 2010, pp. 468–477. | [3] Stuedi, P., Riva, O., and Alonso, G. Enabling social networking in ad hoc networks of mobile phones. Proc. VLDB Endowment, 2009, pp. 1634–1637. | [4] Yao, A. Protocols for secure computations. In Proc. the 23rd Annual Symposium on Foundations of Computer Science, 1982, pp. 160–164. | [5] Agrawal, R., Evfimievski, A., and Srikant, R. Information sharing across private databases. In Proc. ACM SIGMOD, 2003, pp. 86–97. | [6] De Cristofaro, E., And Tsudik, G. Practical private set intersection protocols with linear complexity. Financial Cryptography and Data Security, 2010, pp. 143–159. | [7] Kissner, L., And Song, D. Privacy-preserving set operations. In Advances in Cryptology–CRYPTO, 2005, pp. 241–257. | [8] Ye, Q., Wang, H., And Pieprzyk, J. Distributed private matching and set operations. Information Security Practice and Experience, 2008, pp. 347–360. | [9] Qi, Y., and Atallah, M. Efficient privacy-preserving k-nearest neighbor search. In IEEE ICDCS, 2008, pp. 311–319. | [10] Li, M., Cao, N., Yu, S., And Lou, W. Findu: Privacy-preserving personal profile matching in mobile social networks. In Proc. IEEE INFOCOM, 2011, pp. 2435–2443. | [11] Von Arb, M., Bader, M., Kuhn, M., And Wattenhofer, R. Veneta: Serverless friend-of-friend detection in mobile social networking. In IEEE WIMOB, 2008, pp. 184–189. | [12] Ioannidis, I., Grama, A., and Atallah, M. A secure protocol for computing dot-products in clustered and distributed environments. In Proc. IEEE ICPP, 2002, pp. 379–384. | [13] Dong,W., Dave, V., Qiu, L., and Zhang, Y. Secure friend discovery in mobile social networks. In Proc. IEEE INFOCOM, 2011, pp. 1647–1655. | [14] ZHANG, R., ZHANG, Y., SUN, J., AND YAN, G. Fine-grained private matching for proximity-based mobile social networking. In Proc. IEEE INFOCOM, 2012. | [15] A. Becker, "Bluetooth security & hacks," http://gsyc.es/_anto/ubicuos2/bluetooth security and hacks.pdf. | [16] R. Maheshwari, J. Gao, and S. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in 26th IEEE Conference on Computer Communications (INFOCOM 2007), May 2007. |