ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Security Preserving Friending in Mobile Social Networks

Aditya Waghmare[1], Ashish Kothawade[1], Prajakta Kakade[1], Bhagyashri Markad[1], B. L. Dhote [2]

Student, Department Computer Engineering, College, Sinhgad Institute of Technology, Lonavala, University: Savitribai Phule Pune University, India[1]

Guide, Department Computer Engineering, College, Sinhgad Institute of Technology, Lonavala, University: Savitribai Phule Pune University, India [2]

ABSTRACT-In this paper, we design novel mechanisms, when given a preference-profile submitted by a user, that search persons with matching profilein decentralized mobile social networks. Meanwhile, our mechanisms establish a secure communication channel between theinitiator and matching users at the time when a matching user is found. These techniques can also be applied to conduct privacypreserving keywords based search without any secure communication channel. Our analysis shows that our mechanism is privacy preserving(no participants' profile and the submitted preference-profile are exposed), verifiable (both the initiator and any unmatcheduser cannot cheat each other to pretend to be matched), and efficient in both communication and computation. Extensive evaluationsusing real social network data, and actual system implementation on smart phones show that our mechanisms are significantly moreefficient than existing solutions. As the increasing use of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of peoples' lives. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However in this paper we create a profile matching application which helps user to find the people whose profile best matches with others people. In this paper we propose the security protocol which helps from profiling, and we have tried to increase the privacy so that less information about the user profile is revealed.

KEYWORDS: Privacy preserving profile matching, secure communication, decentralized mobile social networks.

I. INTRODUCTION

Background:

A boom in mobile hand-held devices greatly enriches the social networking applications. Many social networking services are available on mobile phones and majority of them are location-aware. However, most of them are designed for facilitating people connections based on their real life social relationship. There is an increasing difficulty of befriending new people or communicating with strangers while protecting the privacy of real personal information. Friending and communication are two important basic functions of social networks. When people join social networks, they usually begin by creating a profile, and then interact with other users. The content of profile could be very broad, such as personal background, hobbies, contacts, places they have been to, etc. Profile matching is a common and helpful way to make new friends with mutual interests or experiences, find lost connections or search for experts. Some applications help a user automatically find users with similar profile within a certain distance. For example, in the social network Color, people in close proximity (within 50 meters) can share photos automatically based on their similarity. MagnetU matches one with nearby people for dating and friend-making. Small-talks connect proximate users based on common interests. These applications use profiles to facilitate friending between proximate strangers and 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, in this work we focus on proximity-based

DOI: 10.15680/IJIRCCE.2017. 0505119

decentralized mobile social networks (MSN) based on short-range wireless technologies such as Wi-Fi and Bluetooth. However the increasing privacy concern becomes a barrier for adopting MSN. 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 untrusted service provider increase the risk of revealing private information.

Motivation:

As the increasing use of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of peoples' lives. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However in this Report we create a profile matching application which helps user to find the people whose profile best matches with others people. In this Report we propose the security protocol which helps from profiling, and we have tried to increase the privacy so that less information about the user profile is revealed.

Goals and Objective

1. Matching profile content.
2. Provide privacy of user.
3. Recommendation of matching users
4. Optimize the mechanism to reduce the overhead for unmatched users.

II. LITERATURE SURVEY

Survey	Year	Topic Focused	Protocol Used	Advantage	Disadvantage
Ming Li [1]	Apr 2011	Find U- Privacy Preserving Profile matching in MSN	Light Weight protocol	1)Secure under HBC model 2)Easily extended prevent attack 3)Short range control interfaces	1)Usability of profile matching 2)Privacy preserving manage in
Rongzing Lu [2]	March 2013	SPOC: Mobile Healthcare Emergency	Vector Protocol For Third Party	1)Centralized healthcare system distributed 2)Reduce healthcare expenses	1) Performance to find the track 2)Reliability 3)Privacy 4)Security, Related To mobile health care services.
Haojin Zhu [3]	Oct 2009	SMART: Secure multilayer credit based Delay Tolerance Network	Public key Certificate based protocol	1)Effectiveness, Efficiency, Security, Generality 2)education in Transmission cost	1) Traffic and keep trade of each other. 2) Expensive computing cost.
Haojin Zhu [4]	Oct 2008	SLAB: Secure Localization ,authentication and billing scheme for wireless n/w	Third Way Handshake Protocol	1)High mobility security solution low-cost device 2)Highly desired	Difficult to work when Network size is large
Rui Zhang [5]	Sept 2013	Privacy Preserving Profile Matching For Proximity Based MSN	Fine Grained Private Matching Protocol	Facilitate one communication leading Allows employees to discuss ideas. To maintain consider business contacts	1) Possibility for hackers to commit fraud and launch spam and virus attack. 2) Result in lost productivity.

				Improve business on short client advertisement	3)Identify theft
Haojin Zhu [5]	Aug 2013	Fairness-aware the privacy preserving friend matching protocol	Friend Matching Protocol/ Novel Protocol	1)Privacy guarantee 2)Fairness assurance 3) Secure multi-party computation (SML) techniques.	1) Mobile user may face the risk of leaking of their personal information and their location privacy. 2) Existing applications fail to consider hide of users profile.

III. SOFTWARE REQUIREMENT SPECIFICATION

User Classes and Characteristics

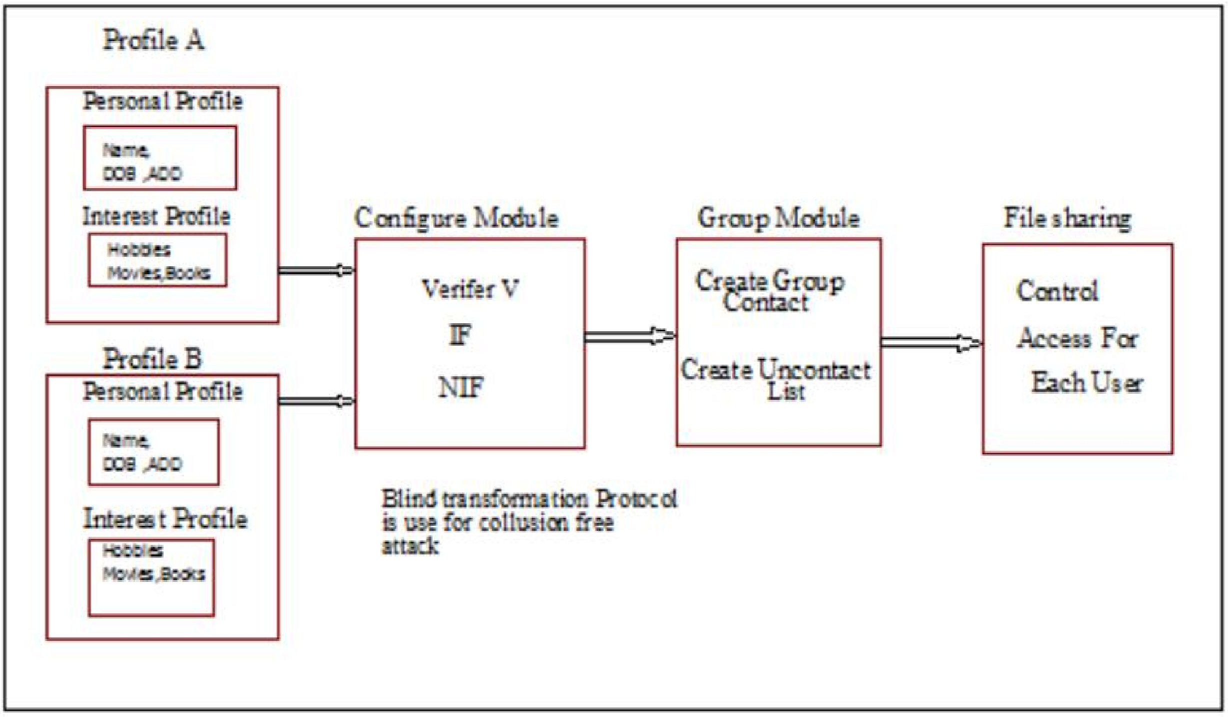
To design products that satisfy their target users, a deeper understanding is needed of their user characteristics and product properties in development related to unexpected problems that the user's faces every now and then while developing a project. The study will lead to an interaction model that provides an overview of the interaction between user characters and the classes. It discovers both positive and negative patterns in text documents as higher level features and deploys them over low-level features (terms).

In proposed work is designed to implement above software requirement. To implement this design following software requirements are used. Operating system: Windows XP/7.

1. Coding Language : JAVA/J2EE
2. Database : MYSQL
3. Tool : Eclipse Luna

IV. IMPLEMENTATION STATUS

The benefitwith the existing Mobile Social Network can get easy access if that person is authorized person. Also the paper suggests that privacypreserving is very sensitive to whether a person is login with their secured ID. So Friend Matching technology isunique in the sense that every person has its unique identity on mobile social networking application. It is different even in the case of identical Twins ID. So to benefit of the technology with the combinationof authentication will be very beneficial as well as secure. Herein above Figure1 Profile A and B created two profilesi.e. Personal Profile having fields Name, Date Of Birth (DOB) and Address and Interest Profile Having fields Hobbies, Movies, Books. Configure Module performing work to match two profile fields to add/ delete each other request. Here modulecontains IF and NIF both interest profile. For comparing, adding and deleting module uses Blind transformation Protocol. Group module creates two lists Group list and rejectedlist. Here whatever the operation performed by software controlled by file sharing, it control access for each other.



V. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

Item	Existing System	Proposed System
Algorithms	Ad Hoc Networks	Advanced Encryption Standard (AES).
Accuracy	Low	High
Complexity	Low	High
Explanation	In the existing system Ad Hoc Networks used not any algorithm	The proposed system is to propose Advanced Encryption Standard (AES) Algorithm. It is found at least six timefaster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow. **Advantages**: • Symmetric key symmetric block cipher • 128-bit data, 128/192/256-bit keys • Stronger and faster than Triple-DES • Provide full specification and design details • Software implementable in C and Java

VI. ALGORITHM FOR RELEVANT FEATURE DISCOVERY

Efficient Algorithms play important role in the relevant feature discovery from text document using text mining. The following steps explain the relevance feature of text documents:
1. Start.
2. Search the matched user.
3. Identify user parameter
3. Share message or communicate to the user
7. Stop

VII. SYSTEM ARCHITECTURE

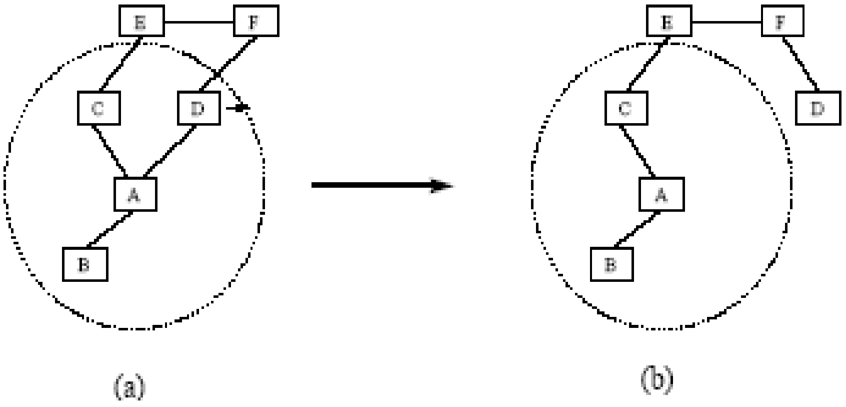


Fig 02 Topology change in Ad Hoc network

Fig shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F.

EXPLANATION-
Nodes A, B, C, D, E and F constitute a mobile Ad Hoc network. The circle represents the radio range of node A. The network initially has its topology in (a) as shown in the fig. When node D moves out of the radio range of node A, the topology changes to as shown in (b) in fig Ad Hoc Networks are useful in areas that have no fixed infrastructure and hence need alternative ways to deliver services. Ad Hoc Networks work by having mobile devices connect to each other in the transmission range through automatic configuration, i.e., setting up an ad hoc network that is very flexible. In other words there is no intervention of any controller that goes ahead and gathers data from all nodes and organizes it. All data gathering and cross-node data transfer is taken care of by the nodes themselves. Ad Hoc Networks are a major goal towards the evolution of 4G (Fourth generation) devices. In the nodes of the Ad Hoc Networks, computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves to find the information or software they need.

VIII. MATHEMATICAL MODULE

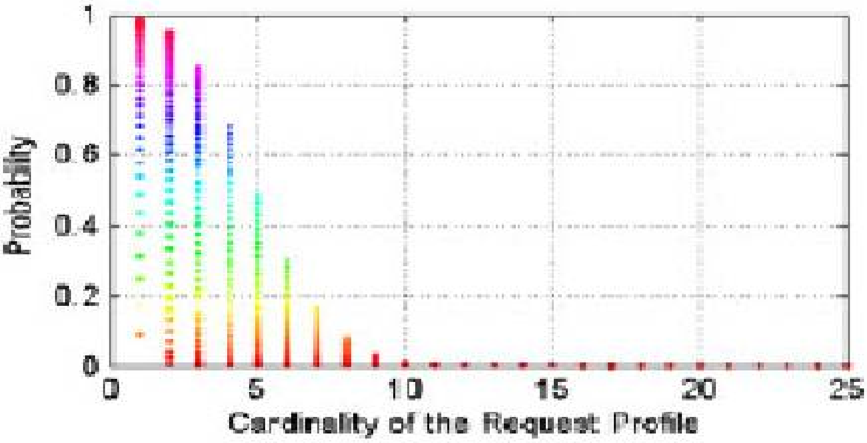
In this module is separate key is created which is the key of the required profile, the initiator scrambles the secret Message Bottleage utilizing a symmetric encryption procedure like Advanced Encryption Standard (AES). Any individual who gets it tries to decode the secret Message Bottleage with his/her own profile key. Just the precisely coordinating individual will decode the Message Bottleage accurately. To protect the profile privacy and support a fuzzy search, a cryptographic hash (e.g. SHA-256) of the attribute is adopted as the attribute equivalence criterion in this mechanism. Assume the cryptographic hash function is H which yields n-bit length hash value. With a sorted normalized profile:

$$A_k = (a_k^1,\ a_k^2,\ a_k^3 \ldots . a_k^m)$$

$$H_k = H(A_k) = (h_k^1, h_k^2,\ h_k^3 \ldots . h_k^m)$$
$$here h_k^i = H(a_k^i,)$$

A remainder vector are designed to significantly reduce the computation and communication overhead of unmatched users the proposed system if efficient and secure in nature. Almost each and every attribute in the system is secured in order to make the user profile private. The profiles and the communication Message Bottleages are secured at database level so that any intruder who gets access to database cannot disclose user’s personal data. The reminder and hint matrix give us the result in shortest span of time.

IX. EXPERIMENTAL SET UP



In this paper we create a profile matching application which helps user to find the people whose profile best matches with others people. In this paper we propose the security protocol which helps from profiling, and we have tried to increase the privacy so that less information about the user profile is revealed.The initiator user allowed his information or any communication to matching user who match the all parameter to decide the initiator.

X. CONCLUSION

In this paper we have surveyed different Profile Matching Techniques for mobile social network; we compared different technique based on their performance as we have studied in the papers. By surveying we have seen that the security of the profile of users is the major issue in profile matching in mobile social network, we have to implement the best technique which is less prone to attacks and requires less communication cost and computation cost.

REFERENCES

1) E. De Cristofaro and G. Tsudik, “Practical private set intersection protocols with linear complexity,” in Proc. 14th Int. Conf. Financial Cryptography Data Security, 2010, pp. 143–159.
2) W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in Proc. IEEE INFOCOM, 2011, pp. 1647–1655.
3) M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, pp. 1–19.
4) V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
5) B. Han and T. Baldwin, “Lexical normalisation of short text messages: Maknsens a# twitter,” in Proc. 49th Annu. Meet. Assoc. Comput. Linguistics: Human Language Technol., 2011, vol. 1, pp. 368–378.
6) I. Ioannidis, A. Grama, and M. Atallah, “A secure protocol for computing dot-products in clustered and distributed environments,” in Proc. IEEE Int. Conf. Parallel Process., 2002, p. 379.
7) Jung, X. Mao, X.-Y. Li, S. Tang, W. Gong, and L. Zhang, “Privacy-preserving data aggregation without secure channel: multivariate polynomial evaluation,” in Proc. IEEE INFOCOM, 2013, pp. 2634–2642.
8) T. Jung, X.-Y. Li, Z. Wan, and M. Wan, “Control cloud data access privilege and anonymity with fully anonymous attribute based encryption,” IEEE Trans. Inf. Forensics Security, 2015.
9) T. Jung and X.-Y. Li, “Collusion-tolerable privacy-preserving sum and product calculation without secure channel,” IEEE Trans. Dependable Secure Comput., 2014.
10) T. Jung, X.-Y. Li, Z. Wan, and M. Wan, “Privacy preserving clouddata access with multi-authorities,” in Proc. IEEE INFOCOM, 2013, pp. 2625–2633.

DOI: 10.15680/IJIRCCE.2017. 0505119