Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 922 – 931

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

An Efficient Profile Matching Protocol Using Privacy Preserving In Mobile Social Network

Kundan Shewale[a]*, Sachin D. Babar[b]

[a,b]*Department of Computer Engineering,*
Sinhgad Institute Of Technology, Lonavala,
Savitribai Phule Pune University, (M.S.), INDIA

Abstract

As we know user profile matching with privacy-preservation in mobile social networks (MSNs) and bring in a family of novel profile matching protocols. We first intend an explicit Comparison-based Profile Matching protocol (eCPM), that runs between parties, initiator, and a responder. It is to propose modified an implicit Comparison-based Profile Matching protocol (iCPM) which allows the initiator to obtain directly 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 open category that is unknown to the responder. The responder prepares two messages in each category, and the initiator can obtain only one message according to the similarity result on a single attribute. Then further, generalize the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex similarity criteria spanning multiple attributes. The secrecy analysis shows all these protocols achieve the privacy of user profiles. Also, the eCPM reveals the similarity result to the initiator, and provides only relative anonymity; the iCPM and the iPPM do not disclose the outcome at all and provide full anonymity (secrecy). It is to analyze the communication overhead and the anonymity strength of the protocols. 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 show that the eCPM+ achieves significantly higher anonymity strength with a slightly larger number of pseudonyms than the eCPM.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Mobile social network (MSN); profile matching, privacy preservation; oblivious transfer; homomorphism encryption.

1. Introduction

Mobile Social cvNetworking is where those with similar interests connect with each other through their mobile/tablet.

* Corresponding author. Tel.: +91 8956561897
E-mail address: shewale_kundan@yahoo.co.in, sdbabar@sinhgad.edu

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.115

They form near communities. For, e.g., Twitter, Facebook, LinkedIn. Social network sites are unique in allowing individuals to connect strangers, but rather that they enable users to clear and make visible their social networks [1]. On many of the large SNSs, participants are not necessarily networking or looking to meet new people; as an alternative, they are primarily communicating with people who are already a part of their absolute social network. Mobile Social Networks (MSN) is a means of transmitting information using a proper mix of voice, and data devices over networks including cellular technology, private and public IP communications. Mobile Social Networking (MSN) refers to the entire enable elements necessary for the involvement (posting and uploading) and consumption (appearance/ experience) of social media across a mobile network [12]. The key to the definition is the user's implicit or explicit choice of network technologies. If the user accesses a community service policy by way of any device; that uses a cellular network, alone or in combination with a commercially accessible wireless network that has access to cellular network operator-owned resources. Mobile community operators and participant are, and can be, prejudiced by the platforms, trends and members of Communities on the Internet [12], [15].

Nomenclature

MSN Mobile Social Networks
SN: - Social Networking Sites.
OSN: - Online Social Network.
ECPM: - explicit Comparison-based Profile Matching
ICPM: - implicit Comparison-based Profile Matching
IPPM: - Implicit predicate-based Profile Matching
TCA: - Trusted Central Authority

2. Related Work

Mobile social networks as up-and-coming social communication platforms have concerned considerable attention recently, and their mobile applications are developed and implemented pervasively. In mobile social networking applications, profile matching acts as a critical step to help users, especially strangers, initialize exchange 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. E-Small Talker automatically discovers and suggests common topics between users for easy conversation. Deliberate e-healthcare cases by proposing a suggestion matching scheme for mobile health social networks. They considered that such matching scheme is important to the patients who have the same symptom to exchange their experiences, mutual support, and motivation with each other[13]. In general, the profile matching can be considered based on the formats of profiles and the types of matching operations. A public profile matching is the FNP scheme [12], where a client and a server computer their connection set such that the client gets the result while the server learns nothing. Later, Kissner et al. [13] implemented profile matching with more operations including set intersection, union, cardinality and over-threshold operations. On the other hand, Ye et al.[4] further extended the FNP scheme to a distributed private matching scheme and Dachman-Soled et al. [5] It is aimed at reducing the protocol complexity. All the above solutions to the set intersection rely on homomorphic encryption operation. In the meantime, other works [7],[8] employed an oblivious simulated arbitrary purpose of implementing their profile matching protocol, where computational & communication effectiveness are enhanced [3] implemented profile matching according to three enhanced privacy levels:

i) Informative the same attribute group of the two users;
ii) Enlightening the size of the same attribute set, and
iii) Revealing the size rank of the common attribute sets between a user and its neighbors.

They consider an honest-but-curious (HBC) opponent model, which assume that users try to study more in order than allowed by inferring from the profile matching results, but directly following the protocol. They apply secure multiparty computation, the Shamir secret sharing scheme, and the homomorphic encryption system to achieve the confidentiality of user profiles.

3. Profile Matching

Profile matching means; two users are comparing their personal profiles and is often the first step towards supportive PMSN. However, it conflicts with users growing privacy concerns about disclosing their personal profiles to complete strangers before deciding to interact with them.[1] The Concept of Profile Matching is as Follows:

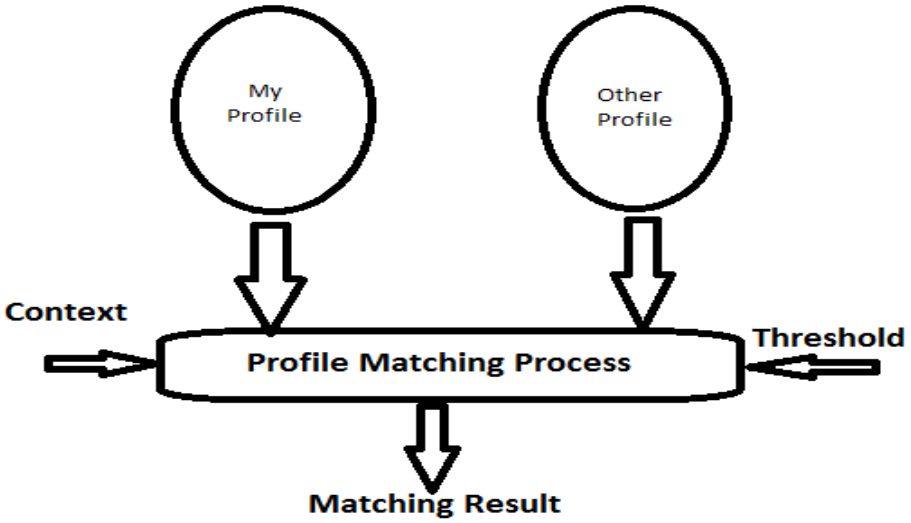


Fig. 1: Process of profile matching

4. Proposal Primitives

A. User Privacy Preservation

The confidentiality is the right to be let alone & it is the right to stay the discovery of personal information safe from others. Privacy implication associated with online social networking depend on the level of identifiability of the information provided; it promises recipient and its possible uses[1][3]. It is comparatively easy for everyone to gain access to it. By joining the network, hacking the site, or impersonate a user by stealing his password. Annoyance to identity theft. Personal data are generously provided and limiting privacy preference is carefully used [12].

B. Homomorphic Encryption

There is several existing homomorphic encryption system that support different operations such as addition and multiplication on ciphertexts. By using these schemes, a user can process the encrypted plaintext, not including meaningful the secret keys. Due to this property, the homomorphic encryption scheme is broadly used in data aggregation and computation purposely for privacy-sensitive content. Here the homomorphic encryption scheme that serve a building block of our future profile matching protocols is reviewed [3,12].

5. Modular Description

After careful examination the system has been identified to have the following modules [8]:

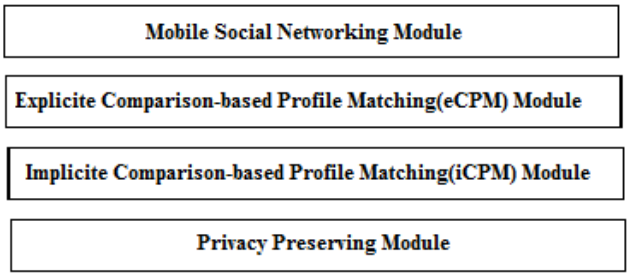


Fig. 2: Modules Of Profile Matching

A. EXPLICIT COMPARISON BASED APPROACH (eCPM)

eCPM protocol allows two users to compare their attribute values on a particular attribute without disclosing the values to each other. However, the protocol reveals the similarity result to the initiator and, therefore, offers relative secrecy (anonymity) [1]. The protocol has a fundamental bootstrapping stage, where the TCA generates all system parameters, user pseudonyms, and key resources.

B. IMPLICIT COMPARISON BASED PROFILE MATCHING (iCPM)

The implicitly based profile matching (iCPM) is proposed by adopting the oblivious transfer cryptographic technique. It is measured that users have separate values for any given attribute. The iCPM consists of three main steps. In the first step, an open category by setting element to 1 and above elements to 0 in a length, vector; Then encrypt the vector by using the homomorphic encryption and send the encrypted vector but still can process the ciphertext. In the second step, computes the cipher texts with the input of self-defined messages for one message length [14].

C. IMPLICIT PREDICTABLE APPROACH (iPPM)

The eCPM & iCPM perform profile matching on a private attribute. For a matching involving multiple attributes, they have to be executing numerous times, each time on one attribute. In this section, the iCPM is complete to the multi-attribute cases, without put at risk its secrecy property, and obtain an implicit Predicate-based Profile Matching protocol, i.e., iPPM. This protocol relies on a predicate that is a logical expression made of multiple comparisons spanning distinct attributes and thus supports various matching criteria within a single protocol run.

6. Three Classes Of Secrecy (Anonymity)

Consider a user has possible instance of the profile

A. Non- Secrecy

A profile matching protocol provides non-secrecy if after executing multiple runs of the protocol with any user, the chance of correctly guessing the profile of the user is equal to 1.[1]

B. Conditional Secrecy

A profile matching protocol achieves relative secrecy if after executing multiple runs of the protocol with some user, the chance of correctly guessing the profile of the user is larger than.[1]

C. Full Secrecy

A profile matching protocol achieves complete anonymity if after executing several runs of the protocol with any user, the likelihood of correctly guess the profile of the user is always[12].

7. The Working Scenario of eCPM is as follows:

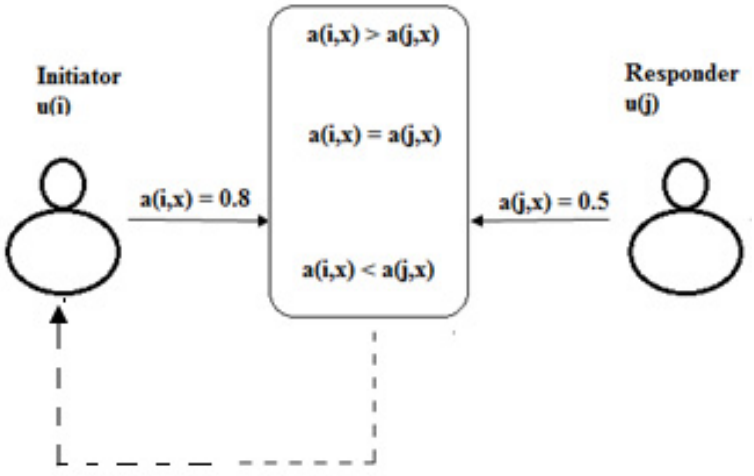


Fig. 3. eCPM working Scenario

Above picture (Scenario) shows: (a) Attribute value ai;x and attribute value aj;x will not be disclosed to uj and ui, respectively. The initiator obtains the comparison result at the end of the protocol. (b) ai;x and aj;x will not be disclosed to uj and ui, in that order. Also, category Ty will not be disclosed to uj , and the comparison result will not be disclosed to any of ui and uj . The initiate or obtains either s1;y or s0;y depending on the similarity result between ai;x and aj;x[14].

Scenario: The initiator wants to know the evaluation outcome, i.e., whether it has a value larger, equal, or smaller than the responder on a specified attribute. For example, as shown in the figure:1, the initiator ui expects to know if ai;x aj;x, ai;x = aj;x, or ai;x aj;x.[8] i.e., eCPM. This protocol allows two users to compare their attribute values on a specified attribute without disclosing the values to each other. However, the protocol reveals the comparison result to the initiator, and, therefore, offers conditional secrecy[12].

8. Flowchart And Algorithm Of Proposed Model [12]:

A. Algorithm:

Step 1: The new user will create a profile.

Step 2: Creating attribute values for the newly created user.

Step 3: Profile creation done.

Step4:

case1: When the user browsed other user's profile, That profile is completely visible to him only when; the majority attribute values match.

case2: If Attribute values do not match the Profile is not completely shown.

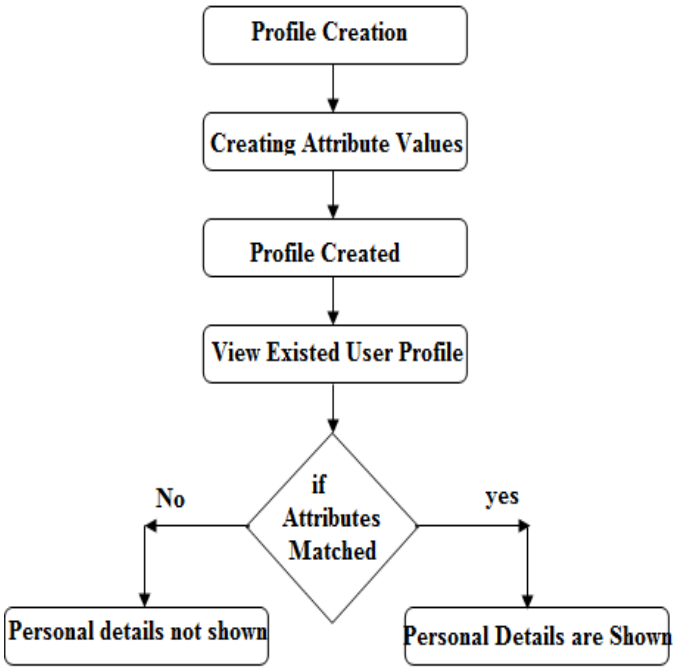


Fig. 4. Flowchart

9. Proposed Framework:

Our goal is to find out the biggest possible number of social profiles that refer to the same person in social networks. To do that, we examine three main areas: social network profile heterogeneity, similarity measuring between attribute values, and decision-making about whether two profiles refer to the same person or not. Here, we propose a framework composed of 4 main components as shown in below figure [8]:

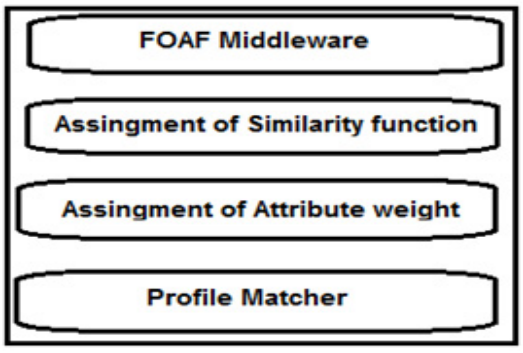


Fig. 5. Framework Proposed

A. FOAF Middleware:

Today's social networks do not accept the same user profile version. It is pinpointed by the "W C Workshop 7" and concluded that most of the technology required to create decentralized social networks exist, such as "RDFa8, Microformats9, XHTML Friends Network (XFN), and Friend of a Friend (FOAF)." Nowadays, FOAF admits to being one of the real sensation stories of the semantic web and is becoming a de facto standard for more and more social networks and kit that agree to generate FOAF profiles. Inveracity, it is a machine-readable semantic vocabulary describing user attributes like people, relationships, and activities. It is write in XML and adopts the conventions of the Resource Description Framework (RDF) to define a set of attributes. A mere example FOAF is provided in Figure 4. We opted to FOAF as a common representation of social profiles and devoted this component to transform the input profiles into FOAF [11,12].

B. Similarity Assignment Function:

Comparing two profiles comes down to compare (a set of) their attributes. To obtain correct results adapted similarity function(s) must be correlated to each attribute (e.g. compare emails must be computed in a different way than comparing interests). A range of techniques can be used to measure the similarity score between two textual/string values and can be group into two broad categories: Syntactic-based similarity approaches: Provide exact or estimated lexical matching of two values. Using exact similarity technique can lead to poor similarity results since numerous variations of a word exist and typing errors are common. Thus, estimated string matching techniques can be used to compute the distance between two values that have a limited instance of different characters. Semantic-based similarity approaches: Used to measure how two values, lexically different, are semantically similar[8]. They can be: Knowledge-based: Computing similarity between values with the usage of predefined (or external) knowledge resources (taxonomies, ontology's, etc.) such as WorldNet, Wikipedia, etc. The similarity can be edge-based (computed following the distance separating values to be compared in the external knowledge) or node based (calculated following the amount of information that a concept contains). Corpus-based: Computing the similarity between two concepts using large corpora only without external knowledge resources. The comparison can be based on vector-space model, statistical such as Pointwise Mutual Information Retrieval, or Latent Semantic Analysis [8][11][12].

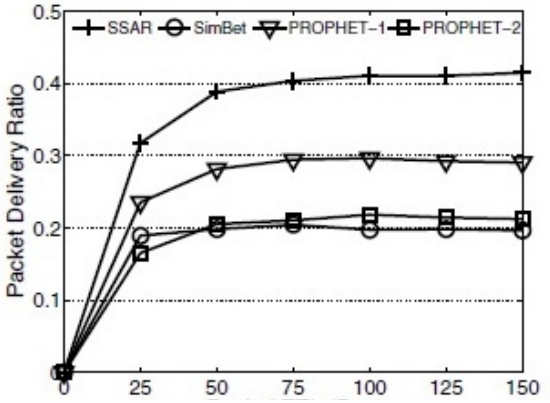
C. Assignment Attribute Weight:

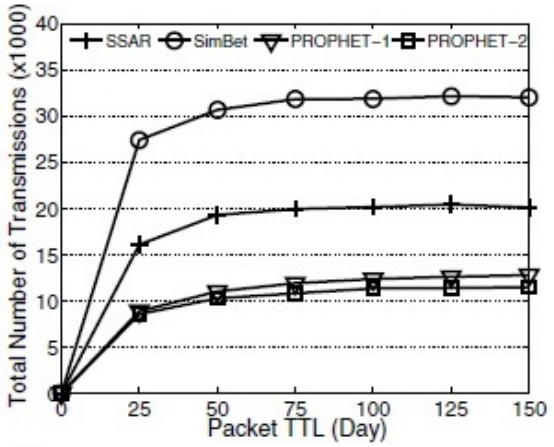
This component principally aims to assign a weight to each attribute in the FOAF expressions. It allows expressive the attribute importance within a defined context. In our structure, the weight can be assigned manually or computed without human intervention. Manual task enables users to include their preferences, and input in the matching process like homepage attributes are more important on LinkedIn than on Facebook) but, the user can use both can start with the automatic assignment and tune it manually after having received the results. In the Automatic assignment; the user gives the framework as input either the list of related social networks or the list of accounts on each social network with the list of IFP attributes12].

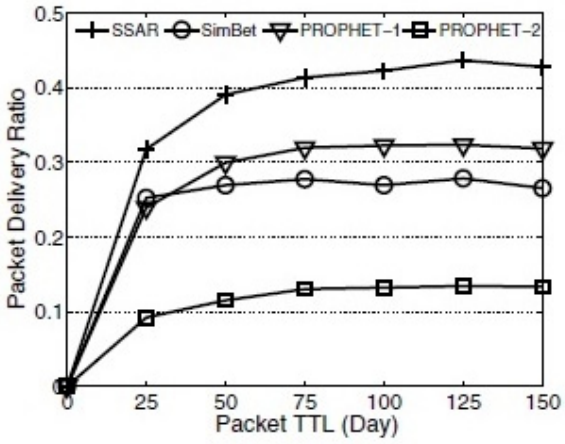
D. Profile Matcher:

This module aims to provide a choice whether two input profiles refer to the same real person or not. Here, two profiles are measured as indicating the same user if their profile match score is higher than a threshold is called the profile matching threshold[15].

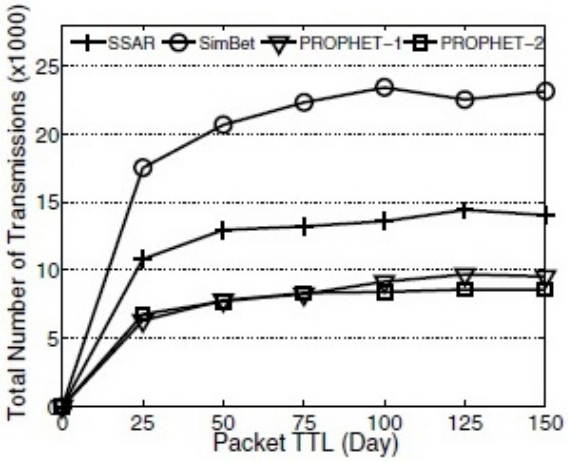
10. Results and Graphs:



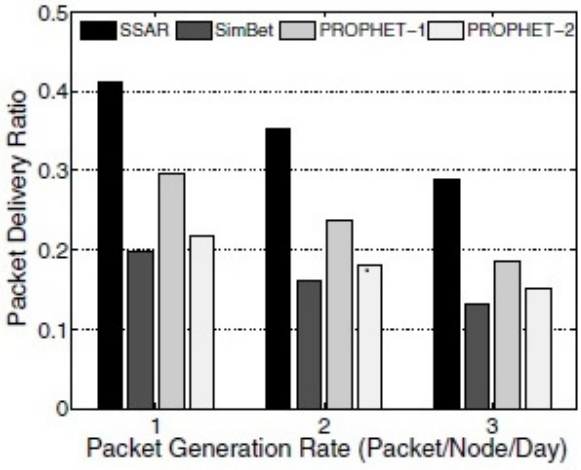




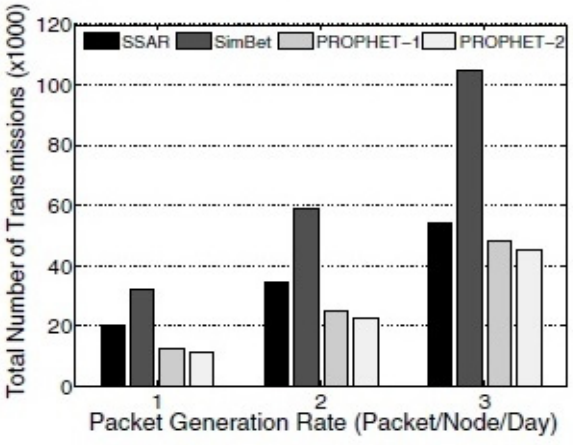
(c) Performance



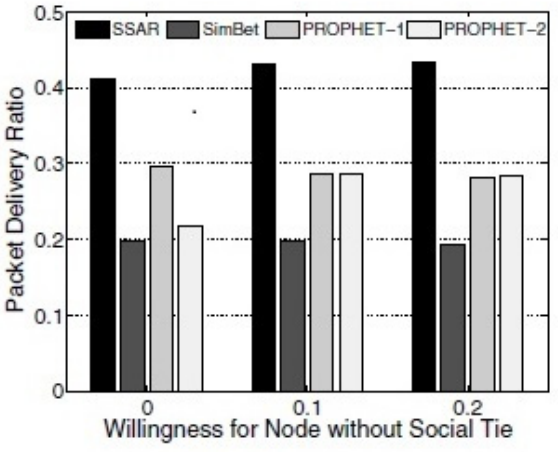
(d) Cost



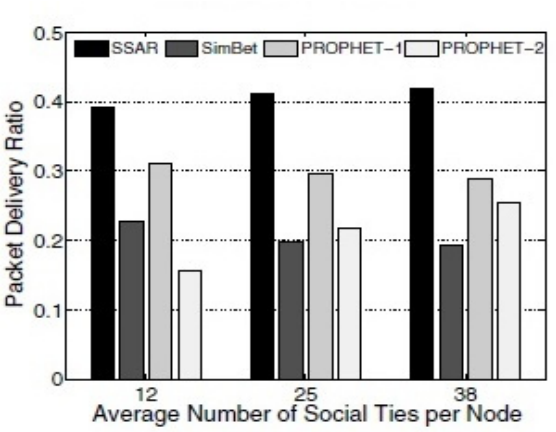
(e) Performance



(f) Cost



(h) Performance



(g) Performance

11. Conclusion:

A distinctive comparison-based profile matching dilemma in Mobile Social Networks (MSNs) is discovered, and original protocols are projected to solve it; The explicit Comparison based Profile Matching (eCPM) protocol provides relative secrecy. It reveals the evaluation result to the initiator. Allowing for the k-anonymity as a user necessity; the anonymity risk level about the pseudonym change for consecutive eCPM is analyzed. Further, an enhanced eCPM+ is introduced, by exploiting the prediction-based plan and adopting the adaptive pseudonym change. The usefulness of the eCPM+ is validated through extensive simulation using real trace data. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM), and implied Predicate-based Profile Matching (iPPM) is implemented. The iCPM handles profile matching based on a single comparison of an attribute; while the iPPM is implemented with a logical phrase made of multiple comparisons across multiple attributes.

References

1. Annet Sahila G, P.Latha, “Privacy Preserving and Fully Anonymous Protocols for Profile Matching in Mobile Social Networks” International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 2, February-2014.
2. Ming Li, Shucheng Yu, Ning Cao, and Wenjing Lou, Senior Member, IEEE Privacy-Preserving Distributed Profile Matching in Proximity based Mobile Social Networks in IEEE INFOCOM 11, Apr 2011.
3. Xiaohui Liang, Xu Li, Kuan Zhang, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, Fully Anonymous Profile Matching in Mobile Social Network in IEEE Transaction On Networking Year 2013.
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.
5. W. He, Y. Huang, K. Nahrstedt, and B. Wu, Message propagation in ad-hoc-based proximity mobile social networks, in PERCOM Workshops, 2010, pp.
6. D. Niyato, P. Wang, W. Saad, and A. Harangues, Controlled coalitional games for cooperative mobile social networks, IEEE Transactions on Vehicular Technology, 18121824, 2011.
7. 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. 22542265, 2012.
8. R. Pradeep, Srinivasa Reddy, CH P. N. V. Mani Kumar, “Preservation in Mobile Social Networks, Science, and Software Engineering”, July - 2014, pp. 440-446
9. R. Lu, X. Lin, X. Liang, and X. Shen, A secure handshake scheme with symptoms matching for mhealthcare social net- work, Mobile Networks and Applications, pp. 112, 2010.
10. C. Zhang, X. Zhu, Y. Song, and Y. Fang, C4: A new paradigm for providing incentives in multi-hop wireless networks, in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 918 926.

11. Elie Raad, Richard Chbeir, Albert Dipanda, “User profile matching in social networks. Network- Based Information Systems” (NBiS), Sep 2010, Japan. pp.297-304, 2014.
12. Xiaohui Liang; Xu Li; Kuan Zhang; Rongxing Lu; Xiaodong Lin; Xuemin Shen, "Fully Anonymous Profile Matching in Mobile Social Networks," Selected Areas in Communications, IEEE Journal on, vol.31, no.9, pp.641-655, September 2013.
13. Wanlei Zhou; Deakin, A., "Keynote Speech VI," in Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on, vol., no., pp.lxix-lxix, 19-21 Dec. 2014 doi: 10.1109/CSE.2014.32.
14. Kolesnikov, Vladimir; Shikfa, Abdullatif, "On the limits of privacy provided by order-preserving encryption," in Bell Labs Technical Journal, vol.17, no.3, pp.135-146, Dec. 2012, doi: 10.1002/bltj.21564.
15. Strunk Jr W, White EB. The elements of style. 3rd ed. New York: Macmillan; 1979.
16. Mettam GR, Adams LB. How to prepare an electronic version of your article. In: Jones BS, Smith RZ, editors. Introduction to the electronic age. New York: E-Publishing Inc; 1999. p. 281-304.