INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 5 ISSUE 3 (2019) PAGES 4379 - 4383
RECEIVED : 12.04.2019 PUBLISHED : 14.05.2019

May 14,2019

# PRIVACY-AWARE INTEREST SHARING AND MATCHING IN MOBOLE SOCIAL NETWORKS

[1] Chaithra B R, [1]Pooja H M, [1]Ranjitha G V, [1]Sindhu H K

[1]UG scholor, department of information science and Engineering

[2]Shashikala S V, Professor & HOD, Dept. of IS&E

[1,2]BGS Institute of Technology, B G Nagar mandya Karnataka.

**Abstract:**

In a profile matchmaking application of mobile social networks, users need to reveal their interests to each other in order to find the common interests. A malicious user may harm a user by knowing his personal information. Therefore, mutual interests need to be found in a privacy preserving manner. In this paper, we propose an efficient privacy protection and interests sharing protocol referred to as PRivacy-aware Interest Sharing and Matching (PRISM). PRISM enables users to discover mutual interests without revealing their interests. Unlike existing approaches, PRISM does not require revealing the interests to a trusted server. Moreover, the protocol considers attacking scenarios that have not been addressed previously and provides an efficient solution. The inherent mechanism reveals any cheating attempt by a malicious user. PRISM also proposes the procedure to eliminate Sybil attacks. We analyze the security of PRISM against both passive and active attacks. Through implementation, we also present a detailed analysis of the performance of PRISM and compare it with existing approaches. The results show the effectiveness of PRISM without any significant Performance degradation.

Keywords - Mobile social networks, interests, profile matchmaking, privacy.

## 1. INTRODUCTION

With the growth of mobile devices and online social networks (OSNs), people can connect with each other ubiquitously anytime. Mobile Social Networks (MSNs) are the emerging trend in mobile technology that combine wireless communication and social networking. MSN inherits advantages of delay tolerant networks (DTNs) and opportunistic networks (Opp-nets) [1]. The main purpose of this paradigm is to provide users with services like location aware services, group texter services, matchmaking services, media sharing services, social gaming, social courier (just to name a few) [1], [17]. One of the popular applications of MSN is profile matchmaking. There are many beneficial application of MSN, where matchmaking can help users to improve themselves, for example in their social life, in finding people with common hobbies and even in health issues. While this is a useful way of finding common interests, matchmaking needs to address a few issues as well. During the matchmaking, a user needs to show his/her interests to other users in order to match their common interests. However, there are various scenarios in which a user may not want to disclose all of his/her interests to other user unless there is the surety that other user has the same interests. Consider a scenario where a patient in a hospital wishes to find someone with the same disease or symptoms he/she is himself suffering from. However, the patient does not want to reveal his disease to anyone else. This kind of scenario makes matchmaking a tricky thing to perform among privacy conscious users .By revealing their private information without a privacy preserving matching mechanism, users put themselves at risk both online (e.g. stalking) and online (e.g. identity theft).

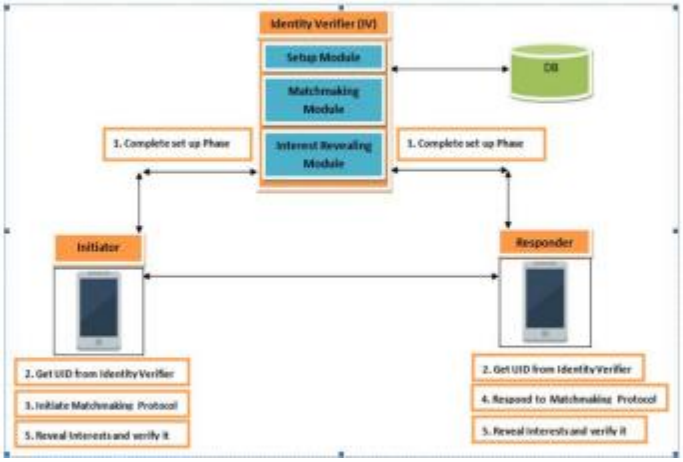
Identity Verifier (IV)
Setup Module
Matchmaking Module
Interest Revealing Module
DB
1. Complete set up Phase
1. Complete set up Phase
Initiator
Responder
2. Get UID from Identity Verifier
3. Initiate Matchmaking Protocol
5. Reveal Interests and verify it
2. Get UID from Identity Verifier
4. Respond to Matchmaking Protocol
5. Reveal interests and verify it

**Fig.1. System Architecture**

Initial setup phase contains initialization of all request from users. It first initiates a request with identity verifier(IV) and identity verifier verifies the request and generates unique id then it provide unique id(UID) to user. With the help of unique id(UID)user can login to their system.

## 2. RELATED WORK

After completion of initial setup phase the matchmaking phase is used to matches the users interest. Following steps shows matchmaking phases working. Alice prepares a matchmaking request that includes her exponentiated interests. Alice then signs the entire message with her secret key and sends this message to Bob. Alice and Bob exchange their matched interests in order to make it sure that both parties have exactly same matches. However, in case anyone of them cheats, the mismatching in the interests will reveal any cheating attempt.

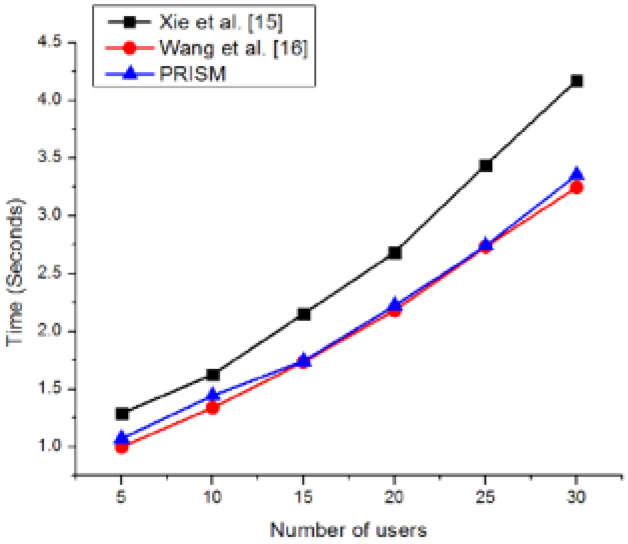

Fig.2

Alice and Bob must have exactly same and equal number of matches. Either they do not have any matched interests or they must have equal number of matches with same interest values. Let p be the number of matched interests at Alice's side and q be the number of matched interests at Bob's side. As mentioned above, P and q are matched interests at both sides and if there is no cheating then p and q must match exactly. It is interesting to note that both Alice and Bob do not know other's matched values. All they know is their calculated values (p in case of Alice and q in case of Bob). Being honest assures Alice as well as Bob that the other value should be same as theirs. We implement PRISM on an Intel i7 CPU with 8 GB of RAM. In order to get average execution time, we ran the experiment for 500 times. We compare the performance of PRISM with approaches presented in [13] and [14]. Moreover, it is worth mentioning that as mentioned in [13] and [14], the execution time of [12] is better due to less number of protocol steps. However, it does not provide mutual interests revealing to both parties and only initiator learns the matched interests. Moreover, [12] is prone to various attacks due to this lack of mutual revealing of interests.

## 3. SYSTEM ANALYSIS

Execution time of [14] is slightly better than PRISM. This is because, this consumption is only based on interaction with a single user. One PKI operation performs slightly better than our proposed exchange of hashes and nonce for interest revealing. However, as the number of users grow, the performance of our protocol in interest revealing phase increased with significant advantage on [14] as shown in Fig. [5]. Fig. 5 presents the execution time comparison by running PRISM against a number of users ranging from 5 users up to 30. The number of interests and number of dummy interests were fixed to 60 and 5 respectively. The graph shows that PRISM outperforms [13] due to the use of Diffie-Hellman, However, PRISM is taking almost similar time with [14]. It is worth mentioning here that, as mentioned earlier, [14] only exchange the matched interests with the best match and therefore, does not exchange matched interests with all the candidates. Therefore, for multiple users,[14] uses one (or few, in case of multiple best matches)expensive PKI encryptions and decryptions. The novel use of hash, in order to share and confirm the matched interests with all the candidates, enables PRISM to execute fast and use dummy interests for more protection without any significant increase in computational cost PRISM is slightly more expensive than both [13] and [14].

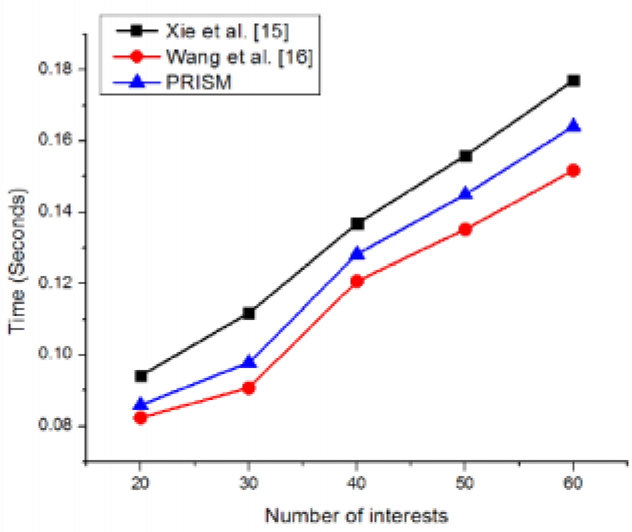

Fig.3.

This is mainly due to the use of dummy interests. However, by considering the fact that PRISM provides much more resilience against the existing approaches, this little overhead can be neglected in practice.

## CONCLUSION

In this, that provide efficient privacy protection and interest sharing protocol in mobile social networks. Here provided novel attacks scenarios and their efficient solution. Unlike existing approaches, PRISM does not require a user to reveal interests to a trusted third party and only uses it as an identity verifier and conflict resolver. The proposed use of unique identity for a user helps prevent Sybil attacks. With the help of implementation that shows the feasibility of PRISM. Moreover, with a comprehensive security and complexity analyses, also show the robustness of PRISM against various attacks as well as its efficiency.

## REFERENCES

[1] Y. Naja_ou, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat, ``Safety challenges and solutions in mobile social networks," IEEE Syst. J., vol. 9,no. 3, pp. 834_854, Sep. 2013.

[2] F. Abbas, U. Rajput, R. Hussain, H. Eun, and H. Oh, ``A trustless brokerbased protocol to discover friends in proximity- based mobile social networks,'in Information Security Applications. Switzerland: Springer, 2014,pp. 216_227.

[3] N. Kayastha, D. Niyato, P.Wang, and E. Hossain, ``Applications, architectures,and protocol design issues for mobile social networks: A survey,"Proc. IEEE, vol. 99, no. 12, pp. 2130_2158, Dec. 2011.

[4] A.-K. Pietiläinen, E. Oliver, J. LeBrun, G. Varghese, and C. Diot, ``Mobi-Clique: Middleware for mobile social networking," in Proc. 2nd ACMWorkshop Online Social Netw. (WOSN), 2009, pp. 49_54.

[5] N. Eagle and A. Pentland, ``Social serendipity: Mobilizing social software,"IEEE Pervasive Comput., vol. 4, no. 2, pp. 28_34, Jan./Mar. 2005.

[6] L. P. Cox, A. Dalton, and V. Marupadi, ``SmokeScreen: Flexible privacycontrols for presence-sharing," in Proc. ACM 6th Int. Conf. Mobile Syst.,Appl. Services (MobiSys), 2007, pp. 233_245.

[7] J. Manweiler, R. Scudellari, and L. P. Cox, ``SMILE: Encounter-based trustfor mobile social services," in Proc. 16th ACM Conf. Comput. Commun.Secur. (CCS), 2009, pp. 246_255.