Privacy Aware Interest Sharing & Matching Protocol in Mobile Social Network

Pawar Gayatri, Borhade Pooja, Borade Ashwini & Wagh Aarati
Students, Department of Computer Engineering, L. G. M. Institute of Eng. Education & Research

Abstract: Mobile social services uses profile matching to help user find friends with similar attributes (For e.g., interest, location, background, etc.).However, privacy concerns often hinder users from enabling this Functionality. In Mobile social network users face the risk of hacking, leaking or expose of their personal information & location Privacy. Based on this, we propose our Privacy Aware Interest Sharing & Matching Protocol, which allows users to match their interest with other without reveal their real interest & Profile & vice versa. To limit the risk of privacy exposure, only minimum information about interest attribute of the users is match with prevention of real profile attributes. It is Secure & almost prevent from hacking profile of users.

Keyword: Profile Matching, Privacy, Online, Social Network

I. INTRODUCTION

Mobile online social network have gained tremendous momentum in the early years due to the increasing of mobile devices like smartphones and tablets as well as pervasive computing availability of network services. So, the technologies like GPS, wireless localization techniques for mobile have made the generation & sharing of real time user location updates available. Location aware mobile social network represent cyber-physical system, which connect mobile devices within local physical proximity by using both smart phones & wireless communication. In Web-based online social networking location-aware mobile social network allow users to have face to face social interaction in public places. Such as airports, trains & Stadiums.

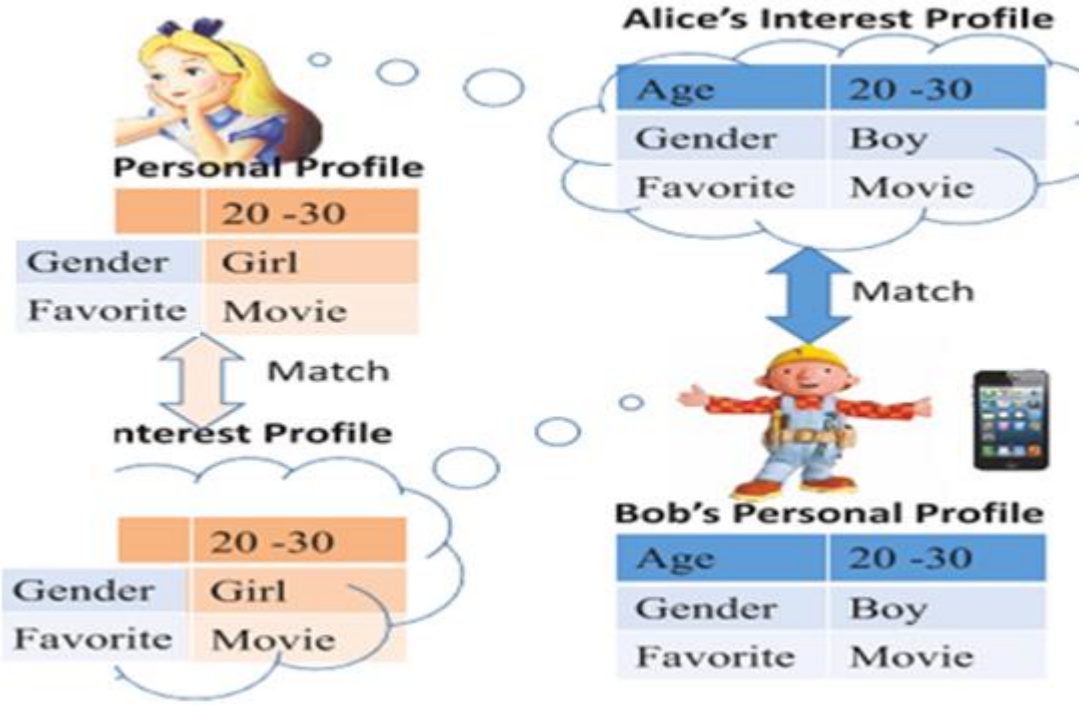

Fig 1. Example of Profile Matching.

Profile matching is important for the wide use of mobile social network. Finding the match able, nearby similar interest is always first prioritize for any social network. The Mobile social network pay limited heed to security & privacy concerns relate with revealing users personal network preferences & friendship information to pervasive computing.

In Mobile Social Network, user face the risk of hacking of their personal information & location privacy. Under this circumstances, attackers can directly associate the personal real profiles with Real user & then do more attacks. Loss of privacy can expose users to unwanted spams, scams, Cause social reputation, damage, and make the victims of blackmail. To prevent these all issues of hacking, leaking & damage we introduce the protocol for it. So, that securely matches the private information of two users. Our Objective is to improve the existing matchmaking protocols & help users to securely perform matchmaking without revealing unnecessary data.

The Main Contribution is:

- Protocol provide a secure & privacy preserving in order to find mutual interest of user.
- Provide effective means to prevent from hammering to users profile.
- These include attacks during matchmaking & interest revealing.
- Provide protection against Sybil attacks by limiting user by at most one device.

Phases:

Initial Setup Phase:

While creating profile on/for social network, mostly user provides their email id, phone number as their unique id. Most of time these Id's guess by our near persons & that causes hacking &Leaking to our personal information. To protect & prevent this our Protocol proposes the use of unique id for mobile as well as for users also.

These unique id for mobile is different for android, ios, windows operating based smartphones.

- Firstly user will create their real profile & interested profile.
- Interest Profile for Matching to prevent the real profile.
- Then the unique id is assign to the user.

Sample Database:

No.	*Username*	*User Id*	*Public Key*	*Secret Key*
1	John Xing	JX123	xyas	@#jx9
2	Alice Desouza	AD456	abcf	%^ad5
3	Shamir	SG789	njlo	@$67

Matchmaking Phase:

Matchmaking means the matching profile.

Basically, Matchmaking Enables Users to discover mutual Interest without revealing their Interests. User will create their own interest that merge automatically as the exponentiated Interest & dummy Interest.

- Public Key: Public key is assign to each user.
- Include sign: Sign is used for Message that is send to other nearby user for Matching Profile.

- Exchange Key: Public key is exchange by users to know the match of profile & interest.
- Attribute Matching: When the message send to user from other user this message include sign, other user verify it, & exchange key then the attributes are match.

Interest Revealing Phase:

For security Purpose to Real profile the other key is generated here. Also value is created. Verification is done here.

- Generate Secret Key: The secret key is generated for security purpose. To prevent the real profile.
- The Hash Value is created here. Hash value includes the User Interest Profile as well as the key.
- Then other user do the same procedure. The keys are exchange by users. Then they find the interest of each other.
- Verification of Attributes: The attributes that are match in Matchmaking phase are verify here. If Interest match then Matchmaking is successful.
- Otherwise, victim Sends protocol records to identity verifier.
- Idv asks the involved participants for the public key, exponentiated interest & hash values. Compare these all. If match with original then ok.
- If doesn't match then Idv erase from its temporary storage to keep privacy.
- Due to Fact that a cheating attempt will be detected immediately.

File Sharing:

If the Matchmaking & Interest Revealing Successful Then Only User Can Share The Files, media, documents, data etc.

System Model:

1) Identity Verifier (Idv): Verifies a legitimate users identification as well as upper limit of his number of interest. Initializes system parameters, also act as dispute resolver. Take necessary action to revoke the malicious users.

2) Initiator: Initiates Protocol by sending interest to other users.

3) Responder: Is the user who replies initiators request by sending his interest for matchmaking.

II. COMPARATIVE STUDY

A. Find U-Privacy Preserving Profile matching in MSN [1]

- Publish Year : April 2011
- Survey : Ming Li
- Architecture Used: Data Sharing, Computation, Reconstruction.
- Protocol Used : Light Weight Protocol
- Algorithm : Shamir's secret sharing, Secure Multiparty

Advantages :

a) Secure under HBC model

b) Easily extended prevent attack

c) Short range control interfaces.

- Disadvantages :

A) Usability of Profile Matching B) Privacy Preserving manage in mobile social network.

B. SPOC : Mobile Healthcare Emergency [2]

- Publish Year : March 2013
- Survey : Rongzing Lu
- Architecture Used :

User community,Privacy Preserving,Key Generation.

- Protocol Used : Vector Protocol For Third Party
- Algorithm : Diffie Hellman
- Advantages

a) Centralised Healthcare system distributed.

b) Reduce Healthcare Expenses

Disadvantages

a) Performance to Find the Track

b) Reliability

c) Security, Related To Mobile Healthcare Services.

C. SMART: Secure multilayer credit based Delay Tolerance Network [3]

- Publish Year : Oct 2009
- Survey : Haozin Zhu
- Architecture Used: System, Encryption, Decryption.
- Protocol Used: Public Key Certificate Based Protocol.
- Algorithm: Blind Transformation Algorithm.
- Advantages :

A) Effectiveness, Efficiency, Security Generality.

B) Education in Transmission Cost.

- Disadvantages :

a) Traffic & keep Trade Of each other.

b) Expensive Computing Cost.

D. SLAB : Secure Localization, Authentication, Billing Scheme for Mobile Social Network [4]

- Publish Year : Oct 2008
- Survey : Haozin Zhu
- Architecture Used: Matching, Devices, Key Encryption, Key Exchange.
- Protocol Used: Third Way Handshake Protocol.
- Algorithm: KNN Algorithm.
- Advantages :

  a) High Mobility Security Solution low- cost devices.

  b) Highly Desired.
- Disadvantages :

  Difficult to Work When Network size is large.

III. CONCLUSION

Our work to develop the system that will ensure the Privacy-Aware Interest Sharing & Profile Matching process in mobile social networks. Future work include how to provide fine grained interest profile matching and investigate more security and privacy issues in mobile social networks.

ACKNOWLEDGMENT

This work is performing under the S. P. Pune University LoGMIEER Computer Department project survey work.

Conflict of Interest: No potential conflict of interest was reported by the authors.

Ethical Statement: The authors declare that they have followed ethical responsibilities.

REFERENCES

[1] W. Dong, V. Dave, L. Qiu, and Y. Zhang, “Secure friend discovery in mobile social networks,” in Proc. IEEE INFOCOM, 2011, pp. 1647– 1655.
[2] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, “On noncooperative location privacy: a game-theoretic analysis,” in ACM CCS, 2009, pp. 324–337.
[3] N. Eagle and A. Pentland, “Social serendipity: mobilizing social software,” IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.
[4] M. Li, N. Cao, S. Yu, and W. Lou, ``FindU: Privacy-preserving personal profle matching in mobile social networks," in Proc. IEEE INFOCOM,Shanghai, China, Apr. 2011, pp. 2435_2443.
[5] W. Dong, V. Dave, L. Qiu, and Y. Zhang, ``Secure friend discovery in mobile social networks," in Proc. IEEE INFOCOM, Shanghai, China,Apr. 2011, pp. 1647_1655.
[6] R. Lu, X. Lin, X. Liang, and X. Shen, ``A secure handshake scheme with symptoms-matching for mhealthcare social network," Mobile Netw. Appl., vol. 16, no. 6, pp. 683_694, 2010.
[7] M. Von Arb, M. Bader, M. Kuhn, and R.Wattenhofer, ``VENETA: Server-less friend-of-friend detection in mobile social networking," in Proc. IEEE WIMOB, Oct. 2008, pp. 184_189.
[8] L. Kissner and D. Song, ``Privacy-preserving set operations," in Advances in Cryptology_CRYPTO 2005, pp. 241_257.
[9] Rongzing Lu, SPOC- A Secure and Privacy Preserving Opportunistic Computing Framework for Mobile Healthcare Emergency March-2013
[10] H. Zhu, X. Lin, R. Lu. Fan, and X. Shen, “SMART: A Secure Multilayer credit based Delay Tolerance Network Oct- 2009

[11] H Zhu. X. Lin,R. Lu, P-H. Ho, and X. Shen, "SLAB: Secure Localized authentication and Billing Scheme for wireless mesh networks," Oct-2008

[12] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, ``Privacy-preserving profile matching for proximity-based mobile social networking," IEEE Sep. 2013.