



Robust Social Recommendation Techniques: A Review

Feng Jiang, Min Gao, Qingyu Xiong, Junhao Wen, Yi Zhang

► To cite this version:

Feng Jiang, Min Gao, Qingyu Xiong, Junhao Wen, Yi Zhang. Robust Social Recommendation Techniques: A Review. 17th International Conference on Informatics and Semiotics in Organisations (ICISO), Aug 2016, Campinas, Brazil. pp.53-58, 10.1007/978-3-319-42102-5_6 . hal-01646558

HAL Id: hal-01646558

<https://inria.hal.science/hal-01646558>

Submitted on 23 Nov 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Robust Social Recommendation Techniques: A Review

Feng Jiang^{1,2}, Min Gao^{1,3}, Qingyu Xiong^{1,3}, Junhao Wen^{1,3}, and Yi Zhang^{1,3}

¹Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University), Ministry of Education, Chongqing 400044, China

²College of Construction Engineering, Chongqing Technology and Business Institute, Chongqing 400052, China

³School of Software Engineering, Chongqing University, Chongqing 400044, China

{jiangfeng, gaomin, xiong03, jhwen, cquzhangyi}@cqu.edu.cn

Abstract. Social recommendation plays an important role in solving the cold start problem in recommendation systems and improves the accuracy of recommendation, but still faces serious challenges and problems. Ratings or relationships injected by fake users seriously affect the authenticity of the recommendations as well as users' trustiness on the recommendation systems. Moreover, the simplification of relationship treatment also seriously affects the recommendation accuracy and user satisfaction to the recommendation systems. This paper first analyzes up to date research of social recommendation and the detecting technology of multiple relationships. Furthermore, it proposes a future research framework for robust social recommendations including modeling and feature extraction of multidimensional relationships, social recommendation shilling attack models based on social relationships, the analysis of the relationships in social networks as well as the roles of relationships on recommendation, and robust social recommendation approaches taking multiple relationships into consideration.

Keywords: Social recommendation, Multiple relationships, Shilling attack

1 Introduction

At present, the rapid development of electronic commerce retail and the rise of social network marketing make social recommendation a research hotspot [1]. Social recommendation refers to recommendation technology taking social relationships as additional input [2] to improve the sales of merchandise and users' satisfaction [1-3].

Social recommendations mainly combine users' social relationships and collaborative filtering technologies [4] to make recommendations. The social relationships between users can be combined with memory-based collaborative filtering method to find nearest neighbor or model-based collaborative filtering as an implicit vector constraints to form memory-based or model-based social recommendation. Social recommendations utilize users' similarities reflected from social relationships [5] to play an important role in solving the cold start problem in the recommendation systems and improve the accuracy of recommendations, but still face serious challenges and problems. First, shilling attacks seriously affect the

authenticity of the recommendation in a social recommendation system [6, 7]. Second, the noise relationship will lead to recommendation failure. There are many relationships in social networks. These relationships are usually dealt with as the same, which is an important reason that explains current social recommendations did not play its due role [8].

Comments injected by fake users seriously affect the authenticity of the recommendation list as well as users' trust degree to the recommendation system; while the simplification of relationship treatment also seriously affects the accuracy of the recommendation list and users' satisfaction to the recommendation system. To solve these issues, the social relationship is a key factor. This paper analyzes up to date research of social recommendation and the detecting technology of interference relationships, as well as proposes a research framework to solve these issues.

2 Social Recommendations and Multiple Relationships Detection

In this section, we will analyze up to date memory-based and model-based social recommendation approaches, fake user detection approaches, and multiple relationship detection approaches because these approaches are essential techniques to robust social recommendation.

2.1 Social Recommendations

Social recommendations usually refer to utilizing social relationships to conduct the merchandise recommendation, conducting the recommendation of friends, micro-blogs, or utilizing celebrities' social influences to conduct the recommendations. The social recommendations in this paper belong to a narrowly-defined social recommendation [9]: a kind of item recommendation technique combining the social relationships. Social recommendation can be divided into memory-based one and model-based one. Memory-based social recommendations directly use ratings and directly linked users as neighbors. Rokach et al. [10] propose a social relationships' weighed average method to find the neighbors. According to the shortest path length from the target user to all users, Golbeck et al. [11] gradually calculate the trust degree and chose those users whose trust values were greater than a threshold value as the neighbor. Jithin et al. [12] use the theory of thermal diffusion for reference to conduct trust transfer in the social relationship networks, meanwhile combined it with traditional rating similarities. Model-based social recommendation takes the model-based collaborative filtering as its foundation, such as the probability matrix decomposition models [15] making relationships between users reflected to preference relationships and achieved the method of social trust integration, the random walk model [13] on social relationships to deal with both positive and negative relationships under the condition of ensuring the convergence and then realize the recommendations, the Social Bayes Personalized Rank (SBPR) model [14]

used in combination with friends' preference to predict ratings, the tensor decomposition model [16] and the multidimensional trust relationship model [17].

These social recommendation approaches utilize users' social relationships and generate effective recommendation as rating matrices are sparse or recommending cold start items. Therefore, the approach can solve the sparsity problem and the cold start problem to some extents; meanwhile improve the accuracy of recommendation. Social recommendation widely drew academia and the industry's attention, but due to a lower cost of establishing social relationships in social networks, social recommendation suffers from the problems related with interference relationships: 1) fake users who improve or lower items' recommendation probabilities by injecting fake users and relationships, which is called the social recommendation shilling attack [6]; and 2) The problem of noise relationship leading to recommendation failure. There are multiple noise relationships that have side-effects on the recommendation, such as temporary friendships or random friendships [18]. If these relationships are treated equally with friendships and colleague relationships, it will make the recommendation results be questioned to a certain extent.

2.2 Social Relationships Detection

Fake user detection. At present, the studies on fake users' interference mainly concentrate on shilling attacks detection in the traditional recommendation systems as well as the methods of detecting fake users in social networks.

In the recommendation systems, Mobasher et al. [19] propose a supervised learning method that used the rating degree mean agreement (RDMA), Degsim, and other features training classifiers to detect fake users. Other researchers [22, 23] put forward a non-supervised learning method based on feature clustering to detect fake users. Cao, et al. [23] raise a semi-supervised learning method which utilized a small amount of labeled data and a large amount of non-labeled data to improve the detection accuracy. Zhang et al. [24] put forward a method to improve recommendation systems' anti-shilling attacks ability by building a users' multi-layered trust model. Wang et al. [25] raise an attack detection algorithm based on target item identification.

In social networks, fake users with the intention of spreading particular contents also can be called "shills" [7] or "water army". The research on fake users in social networks concentrates on that detecting abnormal users based on user features or network structures. Aggarwal et al. [26] extract characteristics from users' registration information, published contents and other information and then built classifiers. Limsaiprom et al. [27] detect fake users by clustering users' source and target addresses.

In social recommendation, Zhang et al. [7] detect fake users based on the cluster of friends' trust relationships. Shrivastava et al. [6] raise that detecting random link attacks by clustering social network diagrams.

Multiple relationship detection. Some research on the multiple relationship are focused on raising problems [8]. Liu et al. [4] believe that social recommendation did not distinguish friendships is one of reasons for its recommendation failure in some case at present. Ghosh et al. [28] raise that in social networks, real users might also build up unreal relationships.

In the aspect of solving the problems, Yeung et al. [18] introduce the concept of relationship strength, and used the method of matrix decomposition and optimization to solve the relationship strength. Tang et al. [17] analyze multidimensional trust relationships based on themes' multidimensional trust tensors and then conducted the recommendation.

3 Analysis and Discussion

At the time of achieving recommendation accuracy and solving the cold start problem, social recommendation is easy to receive fake users' shilling attacks and noise relationships' interference. The detection on fake users in the traditional recommendation system [19, 20, 21], the recommendation based on the calculation of trust degree or target items' abnormality [24, 25] and the detection on fake users in social networks [26, 27] all involved less in the problem of shilling attacks produced when social networks are combined with the e-commerce to conduct product recommendations. In current study on fake users of social recommendation [6, 7], it is assumed that attackers use random link attacks to establish links randomly between fake users and normal users, and if attackers use other strategies to conduct attacks, then it would be difficult to deal with.

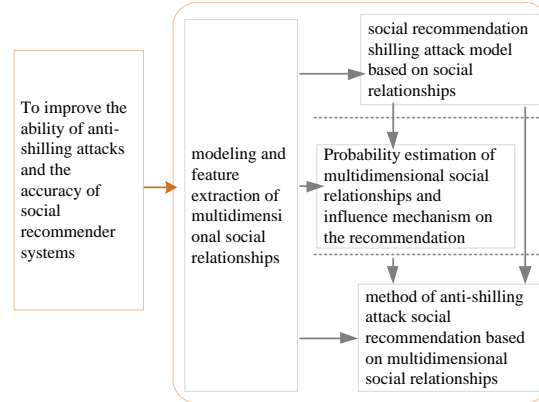


Fig. 1. The Further Research of Robust Social Recommendation

The future research should focus on robust social recommendation, four research points are shown in Fig. 1: 1) The modeling of users' social relationships is the foundation of robust social recommendation. It focuses on the study of using complex network modeling to build fake user injection strategies and shilling attacks models of social recommendation; 2) Utilize the multi-view collaborative training, probabilistic graphical model, tensor decomposition, and other technologies to form the method of probability estimation of multidimensional social relationships; 3) Aim at the cold start, hot and general item exploration to explore function mechanisms of multiple social relationships on the recommendation. The influence of relationships on different types of items can be analyzed by comparing the baseline recommendation algorithms with that by the social recommendation algorithms; and 4) Combine the

multidimensional social relationship probability matrix, and finally build up the algorithm of anti-interference social recommendation to achieve a robust social recommendation system.

4 Conclusion

This paper started from the analysis of the study of social recommendation and existing problems. It explained the characteristic that social recommendation is easy to be attacked by bogus social relationships and be interfered by multiple social relationships. It analyzed the future research point of robust social recommendation, and proposed four aspects: 1) the users' relationship modeling and characteristic extraction faced anti-shilling attack social recommendation; 2) strategies of fake relationship injection and social recommendation shilling attack models; 3) probability estimation of users' multidimensional social relationships and function mechanism of relationship types on social recommendation; and 4) robust social recommendation approaches combined multidimensional social relationships with traditional social recommendation algorithms.

Acknowledgments. This research is supported by the Basic and Advanced Research Projects in Chongqing (cstc2015jcyjA40049), Chongqing University Young Scholar Program, the Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJ121607 and KJ131603) and the Chongqing Social Science Planning Project (2010QNRW54).

References

1. Li, S.S., Karahanna, E.: Online Recommendation Systems in a B2C E-Commerce Context: A Review and Future Directions. *Journal of the Association for Information Systems* 16(2), 72–107 (2015)
2. Tang, J., Hu, X., Liu, H.: Social Recommendation: a Review. *Social Network Analysis and Mining* 3(4), 1113–1133 (2013)
3. Levandoski, J.J., Sarwat, M., Eldawy, A., Mokbel, M.F.: Lars: A Location-Aware Recommender System. *IEEE*, pp. 450–461 (2012)
4. Liu, J., Zhou, T., Wang, B.: Progress in Personalized Recommender Systems. *Progress in Natural Science* 19(1), 1–15 (2009)
5. Gao, H., Tang, J., Liu, H.: Exploring Social-Historical Ties on Location-Based Social Network. *ICWSM*. 2012.
6. Shrivastava, N., Majumder, A., Rastogi, R.: Mining (social) Network Graphs to Detect Random Link Attacks. In: *Proceedings of IEEE 24th International Conference on Data Engineering*, pp. 486–495 (2008)
7. Zhang, X.L., Lee, T.M.D., Pitsilis, G.: Securing Recommender Systems Against Shilling Attacks Using Social-Based Clustering. *Journal of Computer Science and Technology* 28(4), 616–624 (2013)
8. IBM: IBM's black Friday report. <https://strme.wordpress.com/2012/11/27/ibmsblack-friday-report-says-twitter-delivered-0-percent-of-referral-traffic-and-facebooksentjust-0-68percent/> (2012)
9. Ester, M.: Recommendation in Social Networks. *ACM RecSys*, pp. 491–492 (2013)

10. Rokach, L., Shapira, B., Kantor, P.B.: *Recommender Systems Handbook*. New York: Springer (2011)
11. Golbeck, J.: *Generating Predictive Movie Recommendations from Trust in Social Networks*. Springer Berlin Heidelberg (2006)
12. Justin, J., Beegom, A.S.: Nearest Neighbour Based Social Recommendation Using Heat Diffusion. In: *Proceedings of The 6th ACM India Computing Convention*, p. 10 (2013)
13. Chen, Y.C., Lin, Y.S., Shen, Y.C., Lin, S.D.: A Modified Random Walk Framework for Handling Negative Ratings and Generating Explanations. *ACM Transactions on Intelligent Systems and Technology* 4(1), p. 12 (2013)
14. Zhao, T., McAuley, J., King, I.: Leveraging Social Connections to Improve Personalized Ranking for Collaborative Filtering. In: *Proceedings of The 23rd ACM International Conference on Information and Knowledge Management*, pp. 261–270 (2014)
15. Jiang, M., Cui, P., Wang, F., Zhu, W., Yang, S.: Scalable Recommendation with Social Contextual Information. *IEEE Transactions on Knowledge and Data Engineering* 26(11), 2789–2802 (2014)
16. Zou, B., Li, C., Tan, L., Chen, H., Wang, S.: Social Recommendation Based on User Trust and Tensor Decomposition. *Journal of Software* 12(10) 2014
17. Tang, J., Gao, H., Liu, H.: mTrust: Discerning Multi-Faceted Trust in A Connected World. In: *Proceedings of The 5th ACM International Conference on Web Search and Data Mining*, pp. 93–102 (2012)
18. Yeung, A.C.M., Iwata, T.: Strength of Social Influence in Trust Networks in Product Review Sites. In: *Proceedings of The 4th ACM International Conference on Web Search and Data Mining*, pp. 495–504 (2011)
19. Mobasher, B., Burke, R., Bhaumik, R., Williams, C.: Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness. *ACM Transactions on Internet Technology* 7(4), 23 (2007)
20. Wu, Z., Zhuang, Y., Wang, Y., Cao, J.: Shilling Attack Detection Based on Feature Selection for Recommendation Systems. *Acta Electronica Sinica* 40(8), 1687–1693 (2012)
21. Li, C., Luo, Z.: A Metadata-enhanced Variational Bayesian Matrix Factorization Model for Robust Collaborative Recommendation. *Acta Automatica Sinica* 9, 1067–1076 (2011)
22. Lee, J.S., Zhu, D.: Shilling Attack Detection-A New Approach for a Trustworthy Recommender System. *Inform Journal on Computing*, 24(1), 117–131 (2012)
23. Cao, J., Wu, Z., Mao, B., Zhang, Y.: Shilling Attack Detection Utilizing Semi-Supervised Learning Method for Collaborative Recommender System. *World Wide Web* 16(5-6), 729–748 (2013)
24. Zhang, F.G.: Preventing Recommendation Attack in Trust-Based Recommender Systems. *Journal of Computer Science and Technology* 26(5), 823–828 (2011)
25. Wang, H., Yang, W., Wang, S., Li, S.: A Service Recommendation Method Based on Trustworthy Community. *Journal of Computer* 37(2), 301–311 (2014)
26. Aggarwal, A., Almeida, J., Kumaraguru, P.: Detection of Spam Tipping Behaviour on Foursquare. In: *Proceedings of The 22nd International Conference on World Wide Web Companion*, pp. 641–648 (2013)
27. Limsaiprom, P., Tantatsanawong, P.: Social Network Anomaly and Attack Patterns Analysis. In: *Proceedings of The 6th International Conference on Networked Computing*, IEEE, pp. 1–6 (2010)
28. Ghosh, S., Viswanath, B., Kooti, F., et al.: Understanding and Combating Link Farming in the Twitter Social Network. In: *Proceedings of The 21st International Conference on World Wide Web*, ACM, pp. 61–70 (2012)