International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 4, July - August 2016 **ISSN 2278-6856**

A Survey for Efficient and Trustworthy Methods for Detection of Dishonest Recommenders in OSN

Madhura S Khandare[1], Prof. B. D. Phulpagar[2]

[1]Modern College of Engineering, Shivaji Nagar, Pune, India

[2]Modern College of Engineering, Shivaji Nagar, Pune, India

[3]Monash University, Department of Management, McMahons Road, Frankston 3199, Austria

Abstract

Nowadays online social network (OSN) has become crucial part of viral marketing. Some of the popular OSNs can be named as Facebook, LikedIn, Twitter, Flixter in China, etc. Advancement in technology has led to integration of smart phones with OSNs. Using this, many users share their likes, dislikes, opinions, information with their friends in their network. Due to huge popularity of OSN, companies are using target oriented advertisement i. e. viral marketing to publicize or increase the sale of their products. Companies attract small group of users in an OSN and these users provide recommendation to their friends which increases the overall sales of the given product. This also gives chance to spread misleading recommendations to the friends. Therefore, accurate identification of dishonest, misleading users is necessary. Here, glimpse of approaches to detect malicious behaviors of users in OSN, online rating systems, spam detection etc. and their effect on viral marketing have been focused.

Keywords: misleading recommenders, online social networks, spam detection, viral marketing, information security

1. INTRODUCTION

Online social networks (OSNs) are becoming extremely popular since past few years. It is crucial part of viral marketing. Today, technology is so evolved that users can make their purchases online in few clicks through cellphones, laptops, and other smart devices from any location. The impact of OSNs on marketing, advertising cannot be ignored. Companies use viral marketing to boost overall sales of their products. This also leads to misleading recommendations to promote specific product or bad mouth rival product by giving high (low) rating on low (high) quality product. To take advantage of word of mouth effect, firms may also hire some users in online networks to publicize their products. It is of big significance to identify dishonest users and remove them from network to maintain security of viral marketing and to make wise decisions for purchasing products.

There have been a lot of studies that concentrate on information spreading effect in OSN [3], [4]. To maintain the system security, different kinds of works have developed such as trust structures [12], [13], malicious behavior detection in general recommender systems [9], [10], online rating systems [5], [7] and various social networking systems [1]. Fig. 1 depicts general idea of different application domains such as wide OSNs, Online rating systems (OL), General Recommender systems, and their techniques for detection of misleading users in online systems.

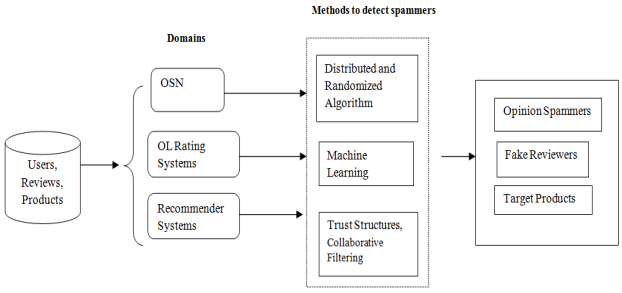

Figure 1. General Scenario of Fake Reviewer Detection

2. RELATED WORK

Here different methods to detect dishonest users in OSN, general recommender system and similar areas where misbehavior of recommenders have been studied. From the view of malicious behavior detection, a lot of work has done such as wireless mesh networks [6], general recommender systems [9], [10] spam detection in Online (OL) rating systems [5], [7], trust structures [12], [13], [14] etc. Figure 1 gives the general overview of different domains in order to identify misleading users in online systems.

Various studies like [3], [4] demonstrate that profit or loss of many business companies get affected due to the viral marketing. Viral marketing is a new strategy exploited by recent corporate firms to promote their products in online

social network platform to increase the sale of the products and get increased financial benefits. Many firms give their product at a much discounted price for the users in OSNs and then they rely on the 'word of mouth effect' in the large OSN platform. Word of mouth effect means spread of opinions for a specific product from user to user in the network. Through this a product may become extremely famous or infamous.

Viral marketing also gives opportunities to misbehave fake recommenders in OSNs. Misleading neighbours may purposefully give wrong recommendations for a right service or product. Companies may also hire such fake reviewers to promote their product or demote the rival product. Therefore, to prevent becoming victim of the dishonest recommenders and get affected on the sales of a company is important.

The work [11] significantly identifies the problem of opinion spamming by studying and analysis of reviews from Amazon.com.

The work [5] review spam detection in OL Rating systems classifies reviews and venues as fake and genuine ones. The paper [7] proposes a novel angle to the problem of opinion spamming by modeling spamicity as latent. Trust structures [12], [13] are used to maintain the system security in delegation and reputation systems computes the trust value for every pair of node in distributed systems.

3. DIFFERENT APPROACHES

3.1 Distributed and Randomized Algorithm in OSN

It presents effective way to identify dishonest recommenders in OSNs [1]. A fully distributed and randomized algorithm is proposed. Users in an OSN can independently apply the algorithm to detect dishonest users from their friend groups. It is based on suspicious set shrinkage. Detection results of neighbors can be integrated to speed up the detection process, thus implementing distributed nature of the algorithm. It also handles network dynamics which means addition of new friends to user's network or sudden deletion or exit of some friends from the network.

3.2 Opinion Spamming using Behavioral Footprints

ASM [7] addresses the problem of opinion spamming. It proposes unsupervised learning approach to identify opinion spamming, in Bayesian setting. This model considers opinion spamming as clustering problem where two clusters exist naturally as spammers and non-spammers. Here, spamicity is latent along with other observed features. Spamicity is the degree of being spam. Reviews of the top ranked and bottom ranked authors are used to build a supervised classifier model.

3.2.1 General overview

It believes spammers have different behavior than non-spammers. Spamicity of every author is latent and each author and review has various behavioral observed features with respect to latent prior class distribution. Model inference understands the latent population distributions of two clusters for two clusters over different behavioral dimensions as well as assignment of clusters of reviews in unsupervised environment based on the principle of probabilistic model based clustering.

3.3 Malicious Review Campaign (Macro)

Macro (Malicious Review Campaign Observer) [5] is a model that identifies the venues which are on the list of attack by the fraudsters. It means that it gives the venues which are affected by malicious behavior of users. At the same time it also makes fraudsters to compromise between their ability to get detected and their influence on the targeted venues. Here, venues depict the businesses, service providers in particular venue, e. g. Car repair and moving companies in San Francisco.

3.3.1 Data

It contributes a dataset which consists of ground truth and gold standard data.

3.3.2 General Overview

It uses social, spatial and temporal information obtained from Yelp website with the help of Ycrawler to classify fake and genuine reviews as well as fraud users and legitimate users.

3.4 Trust Structures

Internet is an example of dynamic network where trust is crucial part for communication, delivery of messages, sharing information etc. [13] is inspired by the trust structures of Carbone, Nelson and Sassones: trust management systems [12]. Universally accepted metric for trust doesn't exist, various metrics are used for their specific purposes [14] proposes a novel trust model for distributed dynamic networks specifically Global Computing. The overall idea of different trust management systems is to calculate the trust value of every node in a network.

3.5 Shill Attack Detection

Shilling attacks [10] are of various types and to prevent such attacks there are several algorithms developed by studying the patterns of these attacks. Different statistical metrics are used to analyze the user rating patterns. Some of these metrics are given bellow:

1. **Number of Prediction Differences (NPD):** For every user in a system, after her exit from system, the number of net prediction changes.

2. **Standard Deviation in User's ratings**: the degree by where user's rating to an item differs from her average ratings.
3. **Degree of agreement with Other Users:** Average deviation in a user's ratings from the average rating of each item.
4. **Degree of Similarity with Top neighbors**: The average similarity weight with the Top-K neighbors of a user.
5. **Rating Deviation from Mean Agreement**: The measure of the deviation of agreement with other users on a set of target items, combined with the inverse rating frequency for these items.

4. CONCLUSION

Different works have been done to detect the fake reviewers in online rating sites, recommender systems and social media. These works majorly implement machine learning algorithms which are further divide into supervised and unsupervised methods. The method distributed and randomized algorithm [1] proposes whole new type of approach to detect misleading recommenders mathematical approach and handles vast amount of data in OSN.

REFERENCES

[1] Y. Li and J. C. S. Lui, "Friends or foes: distributed and randomized algorithms to determine dishonest recommenders in online social networks," IEEE Trans. Information Forensics and Security, vol. 9, October 2014.
[2] https://en.wikipedia.org.
[3] D. Kemp, J. Kleinberg, E. Tardos, "Maximizing the Spread of Influence Through a Social Network", Proc. ACM SIGKDD, pp. 137-1462003.
[4] Y. Li, B. Q. Zhao, J. Lui, "On Modelling Product Advertisement in Large –Scale Online Social Networks," IEE/ACM Trans. Netw. , vol. 20, no. 5, pp. 14121425, Oct. 2014.
[5] M. Rahman, B. Carbunar, J. Ballesteros, G. Burri and D. H. P. Chau, "Turning the Tide: Curbing Deceptive Yelp Behaviors," Proc. SIAM Data Mining Conf. (SDM), 2014.
[6] Y. Li, J. Lui, "Epidemic Attacks in Network-Coding Enabled Wireless Mesh Networks: Detection, Identification and Evaluation", IEEE Trans. Mobile Comput. Vol. 12, no. 11, pp. 22192232, Nov. 2013.
[7] Mukherjee et al., "Spotting Opinion Spammers Using Behavioral Footprints," Proc. ACM SIGKDD 2013, pp. 632640, 2013.
[8] M. Spear, J. Lang et al., "Messagereaper: Using social behavior to reduce malicious activity in networks," Dept. Comput. Sci., Univ. California, Davis, CA, USA, Tech.Rep. CSE-2008-2, 2008.
[9] G. Adomavicius and A. Tuzhilin, "Toward the Next Generation of Recommender Systems: A survey of the state-of-the art and possible extensions," IEEE Trans. Know. Data Eng., vol. 17, no.6, pp. 734749, June 2005.
[10] P.-A. Chirita, W. Nejdl, and C. Zamr., "Preventing Shilling Attacks in Recommender Systems," Proc. of the 7th annual ACM international workshop web information and data management, WIDM 05, pages 6774, 2005.
[11] Jindal, N., & Liu, "Opinion Spam Analysis," International Conference on Web Search and Data Mining (pp. 219–230), 2008.
[12] M. Carbone, M. Nielsen, and V. Sassone, "A Formal Model for Trust in Dynamic Networks" In Proceedings from First International Conference on Software Engineering and Formal Methods, pages 54–61, Sep. 2003.
[13] K. Krukow and M. Nielsen., "Trust Structures" International Journal of Information Security, 6:153–181, 2007.
[14] S. Weeks, "Understanding Trust Management Systems", Proceedings of IEEE Symposium on Security and Privacy, pages 94–105, 2001.

AUTHOR

Madhura Khandare received the B. E. (IT) in 2011 from Jawaharlal Nehru Engineering College, Aurangabad and currently pursuing ME (CS) from Modern College of Engineering Pune.

Prof. B. D. Phulpagar is currently working as Assistant Professor in Computer Engineering Department at P. E. S. Modern College of Engineering Pune (India). He has completed his postgraduate studies at Govt. College of Engineering Pune and Ph. D. in Computer Engineering at Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded, affiliated to Swami Ramanand Teerth Marathwada University Nanded (India).