RESEARCH ARTICLE OPEN ACCESS

Detection of Dishonest Friends in OSN by Efficient and Trustworthy Method

Madhura Khandare [1], Prof. B. D. Phulpagar [2]
Department of Computer Science and Engineering
Modern College of Engineering, Pune
India

ABSTRACT
Today, online social network (OSN) has become integral and important part of human life. The numbers of people using OSN to perform various transactions such as purchasing a product, reviewing different products, internet banking, check ins from specific locations and also the numbers of vloggers, bloggers are increasing day by day. Viral marketing where advertisement of a particular target product for target audience is also emerging with new ideas to promote their products. However, this viral marketing has also given rise to the misleading behavior of some dishonest people to promote and / or demote specific product or rival product for commercial benefit. In OSN vast amounts of users are connected to each other where they give their opinions about different products and services. This paper proposes a method to identify dishonest behaving friends of a user in OSN using combination of mathematical probabilistic approach and machine learning technique.
Keywords :- Online social networks, misleading behavior detection, machine learning.

I. INTRODUCTION

Online social networks (OSN) have become tremendously popular in recent years. Famous examples of OSNs can be given as Facebook, linkedin, Twitter, Instagram, Taobao, etc. These OSNs have attracted enormous number of users. Rapid development in smart phones and their collaboration with OSNs have made it feasible for various users of these services to share information, opinions with their friends. The work proposed here focuses on identifying misleading behaviours of dishonest or false users who purposefully distract users into buying the products or using the services that are not qualified into an intended good category. It proposes a fully distributed and randomized algorithm to detect dishonest recommenders in OSNs.

To elaborate the problem, consider a following example. Suppose a user i in OSN (that user may be in Facebook or Twitter, etc.) wishes to visit a restaurant which provides spicy Indian food and luxurious ambience. This user will seek recommendations from his/her friends from her friend circle in his/her online social network. Based on the maximum number of recommendations from her friends to a particular restaurant, user i will choose to go for that specific restaurant. Thus, opinions of friends in OSNs affect the users' choice of experiencing particular service to a great extent. Therefore, it is necessary to get correct recommendations from the neighbours in our social network to use or buy the products so as to not end up in wrong decisions.

Various studies like [3] 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.

This 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 crucial.

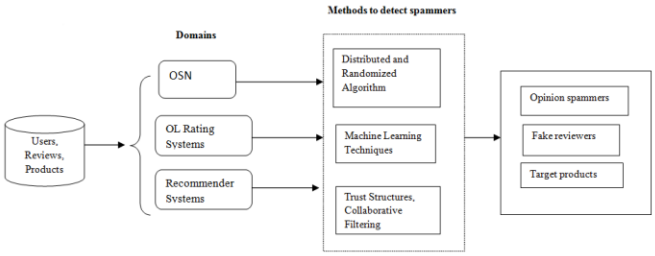


Figure 1. General Scenario of Fake Reviewer Detection

The fig. 1 shows the different application domains such as wide OSNs, Online rating systems (OL), General Recommender systems, Wireless Mesh Networks etc and their respective techniques for detection of misleading users in online systems.

The proposed work uses probabilistic approach and suspicious set shrinkage to detect dishonest neighbours in OSNs. This method derives a set of dishonest friends of a user (detector) and this set is used to train the data for classification into two groups viz. honest and dishonest.

II. RELATED WORK

We review related work and illustrate the difference of detecting dishonest users in OSNs from that in general recommender systems. Many study results [3], [4], [5] state the advantage of word of mouth effect for viral marketing. However viral marketing opens door for malicious behavior as dishonest recommenders can misguide the normal user for their purchases. From the view of malicious behavior detection ,lot of work has done in wireless mesh networks[9], general recommender systems[11], spam detection in Online (OL) Rating systems[7], [8], Trust structures[10].Here we focus the malicious behavior detection in different and wide application scenario i.e. OSNs.

In the aspect of maintaining system security, the work like [1] presents effective way to detect the dishonest recommenders in OSNs. It also handles network dynamics in OSNs. A fully distributed and randomized algorithm to detect dishonest recommenders in OSNs is proposed. It is based on suspicious set shrinkage. In particular, users in an OSN can independently execute the algorithm to distinguish their dishonest neighbors from honest ones. They have further exploited the distributed nature of the algorithm by integrating the detection results of neighbors so as to speed up the detection process.

The work [7] review spam detection in OL Rating systems classifies reviews and venues as fake and genuine ones. They have presented Marco, a system for detecting deceptive Yelp venues and reviews, leveraging a suite of social, temporal and spatial signals gleaned from Yelp reviews and venues. Marco increases the cost and complexity of attacks, by imposing a trade-off on fraudsters, between their ability to impact venue ratings and their ability to remain undetected. It is confined for a limited network. Spam detection techniques generally use machine learning techniques.

The work [8] proposes a novel angle to the problem of opinion spamming by modelling spamicity as latent. In recent years, fake review detection has attracted significant attention from both the business and research communities. However, due to the difficulty of human labelling needed for supervised learning and evaluation, the problem remains to be highly challenging. An unsupervised model, called Author Spamicity Model (ASM), is proposed. It works in the Bayesian setting, which facilitates modelling spamicity of authors as latent and allows us to exploit various observed behavioral footprints of reviewers.

Epidemic attack [9] is a severe security problem in network-coding-enabled wireless mesh networks (WMNs). Malicious nodes can easily launch such form of attack to create an epidemic spreading of polluted packets and deplete network resources. The contribution of this work is to address such security problem. the time-based checksum and batch verification to determine the existence of polluted packets. A set of fully "distributed and "randomized detection algorithms is proposed so that each legitimate node in a WMN can identify its malicious neighbors and purge them for future communication.

Trust structures [11] are used to maintain the system security in delegation and reputation systems computes the trust value for every pair of node in distributed systems. It is costly method to calculate the trust values of every pair of users in OSNs.

The paper [5] considers advertising in viral marketing in large OSN.OSNs are modelled as free scale graphs (either with or without high clustering coefficient).Various influence mechanisms that govern the influence spreading in such large-scale OSNs are employed. The local mean field (LMF) technique is used to analyze these online social networks wherein states of nodes can be changed by various influence mechanisms.

III. PROPOSED METHOD

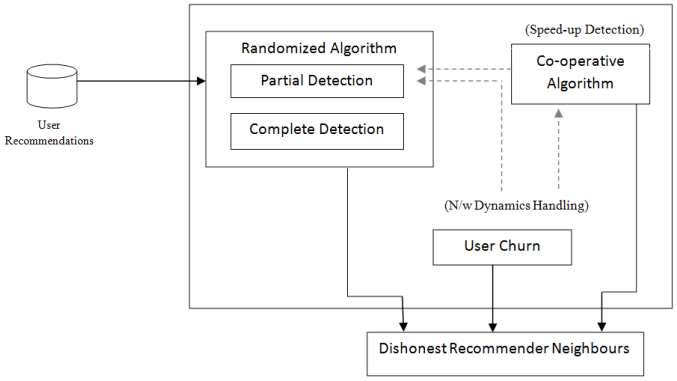


Figure 2: Detection of dishonest recommenders in OSN

The existing system is shown in fig. 2 and fig. 3consists of three methods i. e. Randomized algorithm which is the basic method to categorize the neighbours of user (detector) into suspicious neighbours and non suspicious neighbours, Co-operative algorithm which collects the suspicious set of user and her friends to speed up the detection process and algorithm to handle network dynamics (user churn).

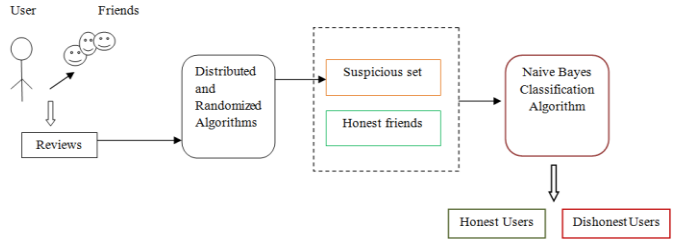


Figure 3.Block Diagram

A. *Processing Steps*

The steps for the proposed systemare given bellow:

1) Randomized Detection Algorithm
2) Co-operative detection
3) Handling Network Dynamics (User Churn)
4) Apply Machine Learning Technique

1) *Randomized Detection Algorithm*

i) Detector 'i' buys a product at round `t', evaluates the product and determines its type as trustworthy product or untrustworthy product.

ii) Receive recommendations from her neighbours and classify those recommendations as correct and wrong recommendations.

iii) Derive suspicious set which contains only dishonest recommenders.

iv) This algorithm is executed iteratively by the user for number of iterations up to some termination condition using predefined probability of false positive.

2) *Co-operative Detection*

i) Exchange the suspicious sets of user and her friends and speed up the detection process of misleading recommenders.

ii) Detector gets the suspicious set by executing randomized algorithm.

3) *Handling Network Dynamics*

i) At any time detector's neighbours in OSN may leave him or her or new friends might be added in the group of detector. This situation is termed as network dynamics and is also called as user churn. This is handled by using the third method which exploits weight of trust values of neighbours of a user in OSN.

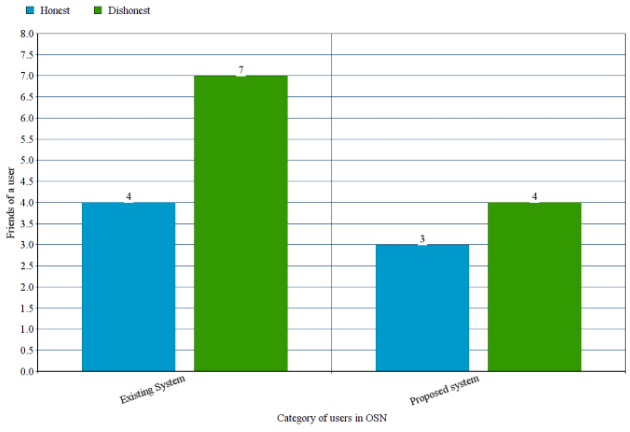
ii) For this user first executes either randomized or co-operative algorithm to get suspicious set.

4) *Apply Machine Learning technique*

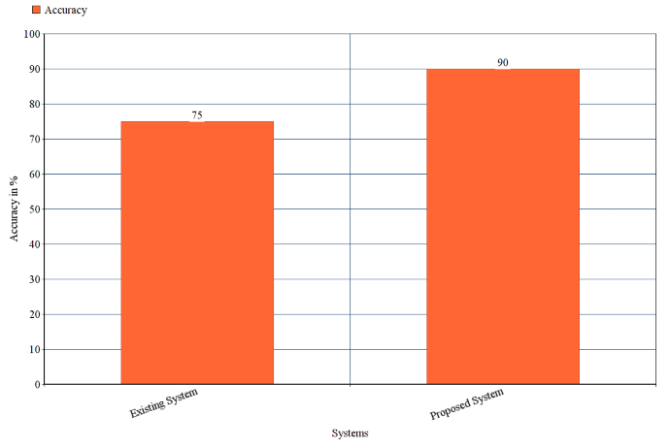
i) Naive Bayes algorithm for classification into honest and dishonest classes is used. Training data consists of the entire already labelled dishonest and correct users list taken from previous results.

IV. RESULTS

The following are the results obtained with the Naive Bayes Classifier algorithm:



Graph1. Classification result



Graph 2. Acccuracy

Here, accuracy is calculated by the formula:

$Accuracy=t_p+t_n/(t_p+t_n+f_p+f_n)$

where,

t_p=true positive

t_n=true negative

f_p=false positive

f_n=false negative

V. CONCLUSION

The detection algorithm distributed and randomized presented here can be viewed as a crucial method to maintain the viability of viral marketing in OSNs.With the help of machine learning technique Naive Bayes, the detection process gives more accurate honest and dishonest neighbours in a network than only using the distributed and randomized algorithms.

ACKNOWLEDGMENT

I take this opportunity to express my deep sense of gratitude towards my esteemed guide Prof. Dr. B. D. Phulpagar for giving me this splendid opportunity to select and present this seminar. I thank Prof. S. A. Itkar, Head, Department of Computer Engineering, for opening the doors of department towards realization of seminar report, all the staff members, for their indispensable support, priceless suggestions and for most valuable time lent as and when required. With all respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

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] T.E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," Proc. IEEE INFOCOM, Apr. 2009

[5] 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.

[6] D. Zhang, H. Xiong, A. Vasilakos, "BASA: Building Mobile Ad-Hoc Social Networks on Top of Android," IEEE Netw. Vol. 28, no. 1, pp. 49, Jan/Feb, 2014.

[7] 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.

[8] Mukherjee et al., "Spotting Opinion Spammers Using Behavioral Footprints," *Proc.* ACM SIGKDD 2013, pp. 632640, 2013.

[9] 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.

[10] 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.

[11] G. Adomavicius and A. Tuzhilin, "Toward The Next Generation Of RecommenderSystems: A survey of the state-of-the art and possible extensions," IEEE Trans. Know. Data Eng., vol. 17, no.6, pp. 734749, June 2005.