ISSN:0975-9646

Sushant Kokate et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3523-3526

Fake Review and Brand Spam Detection using J48 Classifier

Sushant Kokate[1], Bharat Tidke[2]

[1,2]*Department of Computer Engineering, Flora Institute of Technology, Pune, India*

***Abstract*— As the technology changes for publicity, way to traditional marketing also changes as person-to-person communication to online reviews. As feedback these online reviews are important so customer and to companies or vendors. These reviews are helpful for making decisions regarding quality of products and services. Companies and vendors use opinions for making a decision for marketing strategies, performance to services or product, for improvement. However, the intentions to all customers of users are not true for writing reviews. This concepts, changes the face of advertising to conventional, individual-to-individual correspondence to online audits. These online audits are important to client and to organizations or sellers. In this paper we proposed the method to recognizing the untruthful reviews that are given by the users which is having distinct semantic content based on sentiment analysis as the reviews of movies. In this paper author represent to detect the spam untruthful reviews of movies. For this classification we used J48 classifier. We generate ARFF from the distinct features to detecting the untruthful reviews. Using Support Count in Association Rules we further detect Brands in Fake Reviews.**

***Keywords*— Brand Spam detection, Review Spam detection, J48, ARFF, classifier**

I. INTRODUCTION

It is so normal now for e-commerce Websites enabling their customers to write reviews of products that they have purchased. It provides valuable sources of information on these products. So as to used potential customers for finding opinions of existing users before deciding to purchase a product. They also used by product manufacturers to identify problems for their products and to find competitive intelligence information. Author makes an attempt to study review spam and spam detection. To the best of our knowledge, there is no reported study of this problem. Organizations or sellers use reviews to take decisions considering the quality of given products. In any case, all reviews are given by clients users were not given with genuine aim. It is hard for applying any feature for recognize the fake and genuine review.

The context of product reviews, in which opinion are widely used by consumers and product manufacturers. In the past two years, several start up companies also appeared which aggregate opinions from product reviews. It is thus high time for study spam in reviews. Author look here for opinion spam is quite different from the Web spam and email spam, and thus requires different techniques. Based on the analysis of 5.8 million reviews or 2.14 million reviewers from amazon.com, that opinion spam in reviews is widespread. A number of criteria that might be indicative of suspicious reviews and evaluate alternative methods for integrating these criteria to produce a unified 'suspiciousness' ranking. The criteria derive for characteristics of the network of reviewers and so from analysis of the content and impact of reviews and ratings. The integration methods are evaluated are singular value decomposition and the unsupervised hedge algorithm. These alternatives are evaluated to a user study for Trip Advisor reviews, where volunteers were asked to rate that suspiciousness of reviews that are highlighted by the criteria.

Detecting review spam is challenging task as no one knows exactly the amount of spam in existence. Due to the openness of product review sites, spammers pose as different users contributing spammed reviews making them harder so eradicate completely. Spam reviews usually looking perfectly normal until one can compares them with other reviews of same products so as to identify that the review comments not consistent with latter. The efforts of additional comparisons by the users make the detection task tedious and non-trivial. One approach taken of review site such on Amazon.com is to allow users to label or vote the reviews so as helpful or not.

Unfortunately, this still demands to user efforts and is subject to abuse of spammers. The state-of-the-art approach to review spam detection is to treat the reviews as the target of detection. This approach represents review by review-, reviewer- and product- level features, and trains a classifier so as to distinguish spam reviews from non-spam ones. However, these features may provide direct evidence against the spammed review. Both are behaviours of reviewer that to deviate from normal practice and highly suspicious of review manipulation. This suggests that the one should focus on detecting spammers based on their spamming, instead of detecting spam reviews. In fact, the more spamming behaviours we can detect for a reviewer, the more likely the reviewer is a spammer. Subsequently, the reviews to this reviewer can be removed so to protect the interests of other review users. Without doing this the customer is never going to get the quality reviews and thus the decision making will not be an easy task.

II. LITERATURE SURVEY

Here opinion mining attracted to a great deal of research attention. However, the limited work has been done to detecting opinion spam (fake reviews). The problem is analogous to spam in the Web search. However, review spam is harder so as to detect because it is very hard, if not impossible, recognize fake reviews by manually reading them. So find to out a restricted problem, to identifying unusual review patterns which can be suspicious behaviours of reviewers. We formulate the problem as to finding

unexpected rules. The technique is to domain independent. Using the technique, to analysed an Amazon.com review dataset and found many unexpected rules and rule groups which can indicate spam activities.

Consumers increasingly rate, review and research products online [2], [3] (Jansen, 2010; Litvin et al., 2008). Consequently, websites of consumer reviews are becoming targets to opinion spam. While recent work has focused to primarily on manually identifiable instances of opinion spam, in this work so as to study deceptive opinion spam fictitious opinions that have been deliberately written in the sound authentic. Integrating work from psychology and computational linguistics, to develop and compare three approaches to finding deceptive opinion spam, and ultimately develop classifier that is nearly 90% accurate on our gold-standard opinion spam dataset. Based on these feature analysis of our learned models, and additionally make it several theoretical contributions, including a relationship between deceptive opinions or imaginative writing. To detect such attacks unusually correlated temporal patterns. Here to identify and construct multidimensional time series that is based on aggregate statistics, in order so as to depict and mine correlations. In this way, the singleton review spam for detection problem is mapped to abnormally correlated pattern detection problem. To propose hierarchical algorithm for robustly detect these time windows where such attacks are likely to happened. The algorithm also pinpoints such windows in different time resolutions facilitate faster human inspection. So discover that the singleton review is a significant source to spam reviews and largely affects the ratings of online stores.

Now day's large numbers of the product reviews posted to the Internet [6]. Such reviews are important to customers or users and to companies. Customers use the reviews for to deciding quality of the product to buy. Companies and vendors use opinions to take a decision to improve the sales according to intelligent things done from other competitors. All reviews are given by the customers or users are not true reviews. These reviews are given to promote or to demote the product. Some reviews are given on brand of product, and others are related to the advertising of another product. There is need to find out how many reviews are spam or non spam. Here the system is used for detecting untruthful spam reviews using n-gram language model and reviews for brand spam detection using Feature Selection. Given system separately identifies spam and joined the result that showing spam and non spam reviews. For scoring these methods is to measure the degree of the spam for each reviewer and apply them for on an Amazon review dataset. Then to select a subset of highly suspicious reviewers for further scrutiny by our user evaluators with the help of the web based spammer evaluation software specially developed to user evaluation experiments. Then results show that proposed ranking and supervised methods are effective in discovering spammers and outperform other baseline method that based on helpfulness votes alone. Finally here show that the detected spammers have more significant impact on ratings compared with these unhelpful reviewers.

III. PROPOSED SYSTEM

Fig.1 shows basic system structure of proposed system.

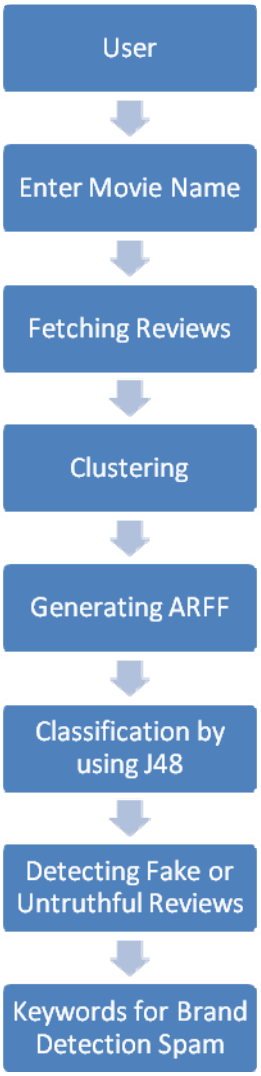

Fig. 1 System Architecture showing all necessary steps in detecting brand spam

The above diagram shows the system representation of the proposed system. Now we will see flow of the system systematically.

1) Initially user enters the name of the movie for obtaining the reviews given by the different reviewers or customers.
2) After entering the name of the movie, API fetches the website of movie review and fetch all the reviews of the movies providing by the websites.
3) After that clustering algorithm is implemented for clustering the reviews in the groups.
4) After completing the process of clustering, the ARFF file is generated, this ARFF file contains the features required for detecting the original reviews and instances of the above attributes. This ARFF contains number of attributes like is question mark present in the review, Capital word in review, polarity, links, comparison, etc.

5) This ARFF file given as a input to the classifier, we used J48 classifier for the detecting the reviews. Training and testing process are done by the J48 classifier.
6) After completing the process of classification, fake and truthful reviews are detected. These reviews now qualify for the further checking for Brand Spam detection.
7) From this review we are removing stop words, after that this review we are putting for the stemming. This reduces the document to a certain level.
8) Now with remaining keywords, we are checking the support count and comparing it with pre decided Threshold Value. Words with support count more than the threshold value will be considered as Brand Spam. Result may retain certain words which cannot be labelled as Brand and it wholly depends on the user or person to judge that through Active Learning.

IV. EXPERIMENTAL STATUS

The experimental setup requires for the proposed system is represented in tabular format. Experimental setup requires minimum configuration given below:

TABLE I
EXPERIMENTAL STATUS

CPU	Intel Pentium IV,2.66 GHz
OS	Windows XP
Memory	512 MB
Storage	10 GB
Technology	JDK 1.7
Tools	Net Beans IDE

A. Result

In the result section we are discussed the results obtained by the system for detecting fake and truthful reviews given by the users.

Following diagram shows the number of reviews of user. In the following diagram, we have fetch total 80 reviews from which the red region shows the truthful review and blue region shows the fake review detected by the proposed system.

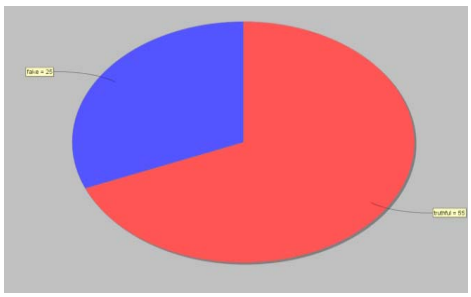

Fig. 2 Average of Truthfulness and Fakeness in Reviews

The following Table. II shows comparative table for all attributes. The comparison is made between J48 and ICRM. True Positive Rate, True negative Rate, Accuracy, Rule, Condition per Rule are the attributes which are considered for comparison.

TABLE II
COMPARATIVE TABLE OF ALL ATTRIBUTES

Confusion Matrix	J48	ICRM
True Positive Rate	97.4	97.5
True Negative Rate	53.3	75
Accuracy	93.4	95.5
Rules	31	7.6
Condition per Rules	3.1	1.9

The following graph 1 shows the comparative results of all attributes:

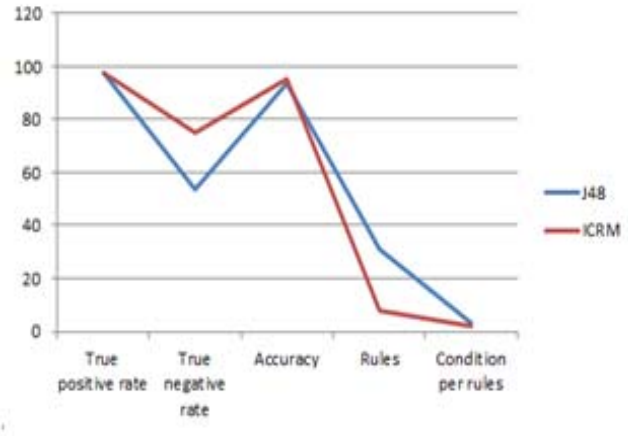

Fig. 3 Comparison Graph of J48 and CRM results

V. CONCLUSION

This paper proposes behavioural approach to detect review spammers who try to manipulate the ratings on some target products. We derive an aggregated behaviour scoring methods for rank reviewers according to the degree that they demonstrate spamming behaviours. So as to evaluate our proposed methods, that conducts user evaluation on an Amazon dataset containing reviews of different manufactured products. We found that here proposed methods generally outperform the baseline method based votes. We further learn a regression model from the user-labelled ground truth spammers. The feedback and viewpoints for decision making is uses by Web users and companies. But these feedbacks are come under the drawbacks like bad publicity and then it is tough to reach right people giving their viewpoints. It becomes mandatory that to detect opinion spam and opinion spammer. This paper focuses on review centric spam detection which provides greater focus on content of feedback. As part of future work, we can incorporate review spammer detection into the review detection and vice versa. Exploring ways to learn behaviour patterns related to that spamming so as to improve the accuracy of the current regression model is also an interesting research direction.

REFERENCES

[1] Nitin Jindal, Bing Liu ,"Review Spam Detection" , ACM Proceedings of the 16th international conference on World Wide Web, pp-1189-1190,2007.

[2] Nitin Jindal, Bing Liu," Opinion Spam and Analysis",ACM Proceedings of the international conference on Web search and web data mining, pp.219-229, 2008.

[3] Guangyu Wu, Derek Greene, Pádraig Cunningham ,"Merging multiple criteria to identify suspicious reviews", Proceedings of the fourth ACM conference on Recommender systems, pp.241-244,2010. M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[4] Nitin Jindal, Bing Liu, Ee-Peng Lim "Finding unusual review pattern using unexpected rules", Proceedings of the 19th ACM international conference on Information and knowledge management, pp.1549-1552,2010. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[5] Myle Ott, Yejin Choi, Claire Cardie, Jeffrey T. Hancock, "Finding deceptive opinion spam by any stretch of imagination" , ACM Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies - Volume 1 , pp.309-319,2011.

[6] Sihong Xie, Guan Wang, Shuyang Lin, Philip S. Yu "Review spam detection via time series pattern discovery", ACM Proceedings of the 21st international conference companion on World Wide Web,pp.635-636,2012. "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[7] Raymond Y. K. Lau, S. Y. Liao, Ron Chi-Wai Kwok, Kaiquan Xu, Yunqing Xia, Yuefeng Li," Text mining and probabilistic modeling for online review spam detection" ACM Transactions on Management Information Systems (TMIS) , Volume 2 Issue 4,Article 25,2011.

[8] Ee-Peng Lim, Viet-An Nguyen, Nitin Jindal, Bing Liu, Hady Wirawan Lauw ,"Detecting product review spammer using rating behaviors", Proceedings of the 19th ACM international conference on Information and knowledge management, pp-939-948,2010.

[9] Guan Wang, Sihong Xie, Bing Liu, Philip S. Yu "Review graph based online store review spammer detection", Proceedings of the 2011 IEEE 11th International Conference on Data Mining, pp.1242-1247,2011.

[10] Arjun Mukherjee, Bing Liu, Junhui Wang, Natalie Glance, Nitin Jindal ," Detecting group review spam" ,ACM Proceedings of the 20th international conference companion on World wide web, pp.93-94,2011.

[11] Arjun Mukherjee, Bing Liu, Natalie Glance ,"Spotting fake reviewer group in consumer reviews", ACM Proceedings of the 21st international conference on World Wide Web, pp.191-200,2012.

[12] Nitin Jindal, Bing Liu, "Analyzing and Detecting Review Spam",Seventh IEEE International Conference on Data Maing,pp.547-552,2007.