IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. V (Jan. 2014), PP 06-09
www.iosrjournals.org

Fake Reviewer Groups' Detection System

Kolhe N.M.[1], Joshi M.M.[2] Jadhav A.B.[3], Abhang P.D.[4]

[1]*(Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune (India))*
[2]*(Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune (India))*
[3]*(Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune (India))*
[4] *(Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune (India))*

Abstract : *We have the cyber space occupied with most of the opinions, comments and reviews. We also see the use of opinions in decision making process of many organizations. Not only organizations use these reviews but also users use them to a great extent. So using this opportunity, many groups try to game this system by providing fake reviews. These reviews enhance or demote the emotions of the products they are acting upon. Many of the organizations pay such groups to promote their product and acquire most of the market share. For a genuine user experience these fake reviews should be detected and deleted. Work had been performed on detecting individual fake reviews and individual fake reviewers; but a fake reviewer group is much more damaging as they take the total control of the product sentiments. This project presents a way to detect these fake reviewer groups. This uses indicators and models to calculate the spamicity of the group. This system deals with detecting fake reviewers' group rather than individual fake reviewers.*

Keywords: *Fake review detection, Group opinion spam, Opinion spam.*

I. Introduction

Expressions can take many forms. The number of people expressing themselves is increasing day by day. In case of internet and the web they take the form of blogs, comments, reviews, forums, journals, etc.
One of the most important forms of expression is reviews. Most of the sites have made it compulsory for their users to post reviews. Reputation of most the restaurants, movies, shops totally depends upon reviews they get from the customers. It has been analyzed that traffic to most of the reviewing sites has increased to 158% last year. This shows how important reviews are. Instead of actually visiting hundreds of customers to record their experience, people find it easier to check out the reviews online. It is found that 97% of people, who made a purchase based on online reviews, found the review to be accurate. What if these reviews are incorrect? There are many cases, in which people either individually or in group, post incorrect reviews about some products. Sometimes these peoples are paid very well.

Such types of spam review can be broadly classified into positive and negative reviews. Positive spam reviews try to promote the products/company they are advertising. This also increases the profit of the product /company. The latter try to malign the product reputation so as to decrease the product sale. The effect is worse, if a negative spam review is written for a good product and positive spam review for a bad product. Both of these spam reviews are harmful in either ways as they totally capture the sentiments of the products, thereby affecting the sale of the product. Such types of reviews should be detected and eliminated to provide users with genuine experience of the business.

In this paper, section 3 summarizes the previous work done in this field. Section 4 provides an idea about our approach in detecting fake reviews. Section 5 and 6 provides a example about the group and individual indicators respectively. Section 7 derives the relational models to be used in the algorithm further. Section 8 provides a look about the algorithm.

II. Need

Reviews are now-a-days very important part of everybody's day to day life. They are useful in many realms of life. E-commerce has become an important sector for reviewing. There are sites specially dedicated for reviewing. Yelp, amazon.com to name a few. Along with the importance of the reviews, the problem of fake reviews also came into picture. The number of fake reviews increased to a greater extent in 21st century as the competition to sustain increased. Many renowned US companies for fined for deliberately posting such reviews. The figure 1 shows an example of fake reviews posted for a hotel in Boston. Following incredulous patterns can be noted in the reviews. (i) Many of the reviewers share the common phrase in the review content. (ii) Most the opinion rating run counter to the majority. (iii) The time when the review was posted, is also leery. Individually, they all appear genuine, but analysis makes it clear that they are not. These reviews clearly have taken the total control of sentiments about the hotel.

In such cases, the truthfulness of the reviews gets hampered. To provide customer with the transparency in the business, such reviews should detected and eliminated..

III. Related Work

Opinion mining and its importance in the decision making process was explored in [1]. The problem of detecting the spam reviews and classifying them was introduced the same. [5] Describes the procedure of detecting the type 1, type 2 and type 3 reviews mentioned in [1]. [3] Mentions the problems associated in detecting the fake reviews. [6] Relates the challenges in Chinese reviews and detecting Chinese spam reviews. Following method of candidate group formation is found accurate. It is described in the following paragraph. **Frequent Item-Set Mining [8]:** We use frequent item-set mining method to form candidate spammer groups from the database. We can use any well-known algorithm for FIM to form candidate groups. By mining frequent Item-sets, we find groups of reviewers, who have reviewed multiple products together. We assume that, minimum support count is equal to 3 i.e. each group must have worked together on at least three products. Groups with support count lower than three are very likely to be due to random chance rather than true correlation. Each group consist of at least two members i.e. two reviewer IDs per item-set.

Fig 1: Fake reviews on a hotel Courtesy: Global staff research

IV. Proposed Architecture

Diagram below represents the proposed architecture of the system, detecting the fake reviews. Input is selected as database file and then processed to detect the product reviews. The spam detection techniques as mentioned in section 5 and 6 are applied to detect any spam in the reviews. The detected spam reviews are then analyzed. This report of analysis is forwarded to the system controller.

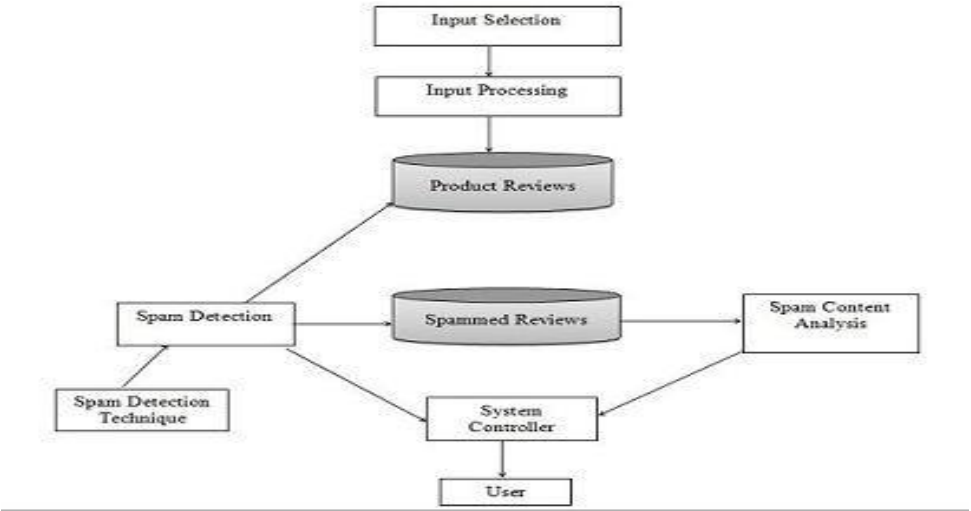

Fig 2: Proposed System Architecture

V. Detecting Parameters

Many criteria can be defined to detect fake reviews. Few of them can be summarized as follows, with each ofthem discussed separately.

5.1 Group Time Stamp**:** Activity of the members of the group is measured over given short interval of time.

Reviews posted within this time period are more likely to be distracting. The latest and the first most dates of review posting are retrieved. It is then normalized on the scale of [0,1]. The relative fakeness can be determined from the value generated.

5.2 Group Rating Fluctuation: Huge difference is found in the rating given by the fake reviewer and the genuine users. This is done to capture the sentiments of the product. The difference is calculated to check for the deviation in the rating in order to know the severity of the group. More the deviation, more damageable the group is.

5.3 Group Plagiarism: Many a times, members of the same group copy the content of the fellow members. This is called as group plagiarism. Duplicate reviews can be detected using this criterion. [6] Showcases Shingle method to detect duplicate and near duplicate reviews. Single method doesn't regard reviews of the same person to the different versions of the product as fake. This drawback is eliminated by using cosine similarity technique to detect plagiarism in the group.

Cosine Similarity: Frequencies of the words in the sentence under consideration is calculated. Consider them as two separate vectors. Hence, we get the similarity between the two vectors which are assumed to be vectors, initially.

5.4 Group Member Plagiarism: Sometimes it is not possible to copy the reviews of the fellow group members, so the reviewer copies his/her own reviews written previously. This is another type of plagiarism exhibited in a group. Again the concept of cosine similarity is used to determine the degree of similarity.

5.5 Early Time Stamp: In order to make more impact, reviewers try to post reviews as soon as the product is released. The time stamp of few months is assumed. After those many months, reviews are not considered to be early.

5.6 Group Impact: It is observed that impact of group is negligible, when genuine reviewers are more in number. It is obtained by taking ratio of spammer groups' size upon total number of reviewers for the product.

5.7 Group Member Impact: This parameter is used to calculate the impact of the group and its members relative to other group, present in the environment.

5.8 Support Count: The likeliness of the group having reviewed many products together is less. If this likeliness comes out to be higher, then it can be added into the stack of fake reviews. This likeliness if described in this parameter.

5.9 Review Length: Some reviews are written just to influence the rating of the product. The content of the review is just a formality. Such types of reviews also can be placed in the set of spam reviews.

5.10Reviewer Investigation: Sticking to the basic definition of the reviewer as reviewers are the people, who have purchased the given product. Genuine reviewer will post the review, if he/she has actually used it.

5.11Stupidity: This can be considered as a surplus criterion for detecting the fake reviews. Reviews written in caps can be considered as a stupid activity and can be ignored.

VI. Individual Spam Detecting Criteria

Group detecting criteria detects the spam reviewer groups. Following are the criteria to detect individual spam activities of members of the group. We define the individual detecting criteria in the context of group detecting criteria.

a. Individual Fluctuation*:* Similar to the group rating fluctuation, the review rating fluctuation is calculated over a given scale of deflection for each member of the group.

b. Content Plagiarism: The content of the individual member is investigated for any content plagiarism for a given product. This is done by using the cosine similarity used in detecting the group plagiarism.

c. Individual Time Stamp: The posting time of the reviews by a given member for a particular product is calculated over a given time stamp is deduced.

d. Individual Coupling: Coupling of the individual member of the group is measured. Earliest and latest dates of the review posting are fetched.

VII. Relational Models

By using above group detection parameters spam and non-spam groups are detected. We derive effective models, which give inter-relationship among products, groups and group members to compute spamicity in further algorithm. Three binary relations are derived as follows.

a. Group spam-Product Model (GPM): This relational model provides us with the relation between group and the products they have spammed. The extent depends upon the spamicity of the group and the extent to which these products were spammed.

b. Member Spam-Product Model (MPM): Here we calculate the spam contribution of the group members individually. Spam contribution of group is equal to the summation of the spam contribution of each of its

member. Individual spam detecting criteria are used here for the calculation.
c. Group Spam-Member Spam Model (GSMS): Group with high spamicity members in it, have overall spamicity as high. High spamicity of group will affect the spamicity of its individual members. This is calculated by using coupling criteria.

VIII. The Algorithm

The scoring algorithm uses the three relational models.
1. Choose the database to be analyzed.
2. Form the candidate groups using the process of Frequent Item set Mining (FIM) method, mentioned earlier. We will have candidate groups formed at the end of this step.
3. Determine the values of the indicators for each candidate group separately. Both, individual and group indictor, values should be calculated.
4. Calculate the values of behavioral models using indicator values from the above step.
5. Now. Calculate the score of each candidate group. Following steps should be iterated until all the groups are covered.
a. Consider the initial spamicity of each candidate group be 0.5.
b. Deduce the initial spamicity of member and product using GPM model and MPM model. c. Using GSMS model, redefine spamicity of group and member.
6. Rank each candidate group according to the score of the spamicity, using any sorting algorithm.

IX. Conclusion

This paper proposes to detect fake reviewer groups'. We found that spotting the individual fake reviews was quite a difficult task but spotting the groups' was comparatively easier one. We propose the scoring algorithm which consists of three models which are used to analyze the dataset and form the candidate groups using the process of Frequent Item set Mining (FIM)[8] method and we also proposed some behavioral features which are considered for finding fake reviews.

Acknowledgement

We express our thanks to the all those who have provided us valuable guidance towards the planning of this system. Nevertheless, we would like to thank to our families for encouraging us and for their support.

References

[1] Amir A. Sheibani IST' 2012.Opinion mining and opinion spam. Shiraz University.
[2] Nitin Jindal and bing liu 7th IEEE ICDM. Analyzing and detecting review spam. University of illinios, Chicago.
[3] Yingying ma and fengjun li. 8th ICCC. Detecting review spam: challenges and opportunities. The University of Kansas, Lawrence.
[4] C.L. lai, K.Q. Xu, Raymond Y.K. lau, City University of Hong Kong, Y. Li Queensland University ofTechnology, L. Jing Beijing Jiaotong University, China. IEEE ICEBE. Towards a language modeling approach for consumer review spam detection.
[5] Siddu P. Algur, Amit P. Patil, P.S. Hiremath, S. Shivashankar. Conceptual level similarity measure based review spam detection. B.V. Bhoomaraddi College of engineering and technology, hubli, Karnataka, India.
[6] Yahui Xi, Tianjin, China. 2012 ICCECT. Chinese Review spam classification using machine learning method. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.
[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE. [8]Arjun Mukherjee, Bing Liu, Natalie Glance. Spotting fake customer reviews in consumer reviews.
[9] Chirita, P.A., Diederich J. and Nejdl, W.MailRank: Using Ranking for spam detection. CIKM, 2005.