International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Spam Review Detection and Removal in E-Commerce Website

D. Janupriya[1], S. Vallimayil[1], N. Sujanthini[1], V. Nandhini[1], A. T. Barani Vijayakumar[2]

[1]B.E Scholar, Department of Computer Science and Engineering, Saranathan Engineering College, Panjapur, Trichy, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science and Engineering, Saranathan Engineering College, Panjapur, Trichy, Tamil Nadu, India

ABSTRACT

In this era, most of the people are eager to purchase products via online e-commerce sites such as Flipkart, Amazon, Paytm., etc. Before purchasing any products via online people spend some time for analyzing the available comments such as feedbacks, reviews and ratings related to the product which are posted by other customers. Based on these comments, people took a decision whether to buy that product or not. If the given comments are positive, then there is a chance to buy the product. If not, people may ignore the product. On the other hand, these reviews play a vita role in the improvement of a business. Positive reviews can add profit to a company. While negative reviews can potentially impact credibility and cause economic loss to a company. For gaining profit to a company or making a company reputation down, imposters namely spammers were encouraged to write fake reviews about a company product. These fake reviews can mislead the customers in taking decision. If the fake reviews are positive, then most of the customers trust them and buy the product there by improve a company profit rate. Where as in case of negative reviews, the customers won't buy the product there by damage the reputation of a company. Therefore, it is most important to detect the spammer and spam content to make online purchase trustworthy. In the past few years, several approaches have been proposed to deal with the problem but there are still some millstones for detecting the spammer and spam content correctly. The proposed framework includes two methodologies namely, Rate Deviation using Threshold and User Behavioral method for identifying spammer and spam contents in an effective manner. In Rate Deviation using Threshold method, it calculates a score value against each user rating and overall rating of a product. Whereas in User Behavioral method, it calculates the user burst time.

Keywords: E- Commerce Site, Spammer, Spam Content, Positive Review, Negative Review, Score, Threshold, Burst Time.

I. INTRODUCTION

With the development of the Internet, people are more likely to express their views and opinions on the Web. In the present scenario, customers are more dependent on making decisions to buy products either on ecommerce sites or offline retail stores. There are number of users who use these commercial websites to buy products online because of their comfort. Most of the E-commerce sites provide review section for users so that they can post reviews of products at merchant site and express their views. So as to used potential customers for finding opinions of existing users before deciding to purchase a product. These opinions are also used by product manufacturers to identify problems for their products and to find competitive intelligence information. Such content contributed by web is called as user-generated content. This content forms valuable information for merchants other customers, product

manufacturers. Though these reviews are important source of information there is no quality control on this user generated data, anyone can write anything on web which leads to many low quality reviews still worse review spam which mislead customers affecting their buying decisions.

Trusted customer reviews are useful for both potential buyers and product manufacturers. It is more convenient and less time consuming for buyer to see at a glance feature by feature comparison of reviews written by most of the customers in taking buying decisions without getting biased. 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. Since reviews are game changers for success or failure in sales of a product, reviews are being manipulated for positive or negative opinions. Manipulated reviews can also be referred to as fake/fraudulent reviews. In today's digital world opinion spam has become a threat to both customers and companies. Distinguishing these fake reviews is an important and difficult task. As a result, it is a herculean task for an ordinary customer to differentiate fraudulent reviews from genuine ones, by looking at each review. So, there is a great need to develop a new approach that works to detect spam in e-commerce website. No stand alone statistical analysis can assure that a particular review is fraudulent one. It can only indicate that this review is more likely to be suspicious. Detection and filtering of genuine reviews is an interesting problem for e-commerce sites. In this work we try to detect and block the spam reviews from spammers in e-commerce website.

II. LITERATURE SURVEY

2.1 Harnessing the power of multiple review sites[2] .

Description

Online reviews on products and services can be very useful for customers, but they need to be protected from manipulation. So far, most studies have focused on analyzing online reviews from a single hosting site. How could one leverage information from multiple review hosting sites? This is the key question in our work. In response, we develop a systematic methodology to merge, compare, and evaluate reviews from multiple hosting sites.[2] We focus on hotel reviews and use more than 15 million reviews from more than 3.5 mil- lion users spanning three prominent travel sites. Our work consists of three thrusts: (a) we develop novel features capable of identifying cross-site discrepancies effectively, (b) we conduct arguably the first extensive study of cross-site variations using real data, and develop a hotel identity-matching method with 93% accuracy, (c) we introduce the True View score, as a proof of concept that cross-site analysis can better inform the end user. Our results show that: (1) we detect 7 times more suspicious hotels by using multiple sites com- pared to using the three sites in isolation, and (2) we find that 20% of all hotels appearing in all three sites seem to have low trustworthiness score. Our work is an early effort that explores the advantages and the challenges in using multiple reviewing sites towards more informed decision making.

DISADVANATGES

- ✓ Less effective in target identification
- ✓ Unreliable performance

2.2 Towards detecting anomalous user behavior in online social networks[3].

Description

Users increasingly rely on crowd sourced information, such as reviews on Yelp and Amazon, and liked posts and ads on Facebook. This has led to a market for black hat promotion techniques via fake (e.g., Sybil) and compromised accounts, and collusion networks [3]. Existing approaches to detect such behavior relies mostly on supervised (or semi-

supervised) learning over known (or hypothesized) attacks. They are unable to detect attacks missed by the operator while labeling, or when the attacker changes strategy. We propose using unsupervised anomaly detection techniques over user behavior to distinguish potentially bad behavior from normal behavior. We present a technique based on Principal Component Analysis (PCA) that models the behavior of normal users accurately and identifies significant deviations from it as anomalous. We experimentally validate that normal user behavior (e.g., categories of Facebook pages liked by a user, rate of like activity, etc.) is contained within a low-dimensional subspace amenable to the PCA technique. We demonstrate the practicality and effectiveness of our approach using extensive ground-truth data from Facebook: we successfully detect diverse attacker strategies—fake, compromised, and colluding Facebook identities—with no *a priori* labeling while maintaining low false-positive rates. Finally, we apply our approach to detect click-spam in Facebook ads and find that a surprisingly large fraction of clicks are from anomalous users.

DISADVANATGES

- ✓ Low efficiency
- ✓ Unreliable detection of spams

2.3 Spotting fake reviews via collective PU learning[4].

Description

Online reviews have become an increasingly important resource for decision making and product designing. But reviews systems are often targeted by opinion spamming[4]. Although fake review detection has been studied by researchers for years using supervised learning, ground truth of large scale datasets is still unavailable and most of existing approaches of supervised learning are based on pseudo fake reviews rather than real fake reviews. Working with Dianping1, the largest Chinese review hosting site, we present the first reported work on fake review detection in Chinese with filtered reviews from Dianping's fake review detection system. Dianping's algorithm has a very high precision, but the recall is hard to know. This means that all fake reviews detected by the system are almost certainly fake but the remaining reviews (unknown set) may not be all genuine. Since the unknown set may contain many fake reviews, it is more appropriate to treat it as an unlabeled set. This calls for the model of learning from positive and unlabeled examples (PU learning). By leveraging the intricate dependencies among reviews, users and IP addresses, we first propose a collective classification algorithm called Multi-typed Heterogeneous Collective Classification (MHCC) and then extend it to Collective Positive and Unlabeled learning (CPU). Our experiments are conducted on real-life reviews of 500 restaurants in Shanghai, China. Results show that our proposed models can markedly improve the F1 scores of strong baselines in both PU and non-PU learning settings. Since our models only use language independent features, they can be easily generalized to other languages.

DISADVANATGES

- Low performance on detection
- False prediction of reviews

3. PROPOSED SYSTEM

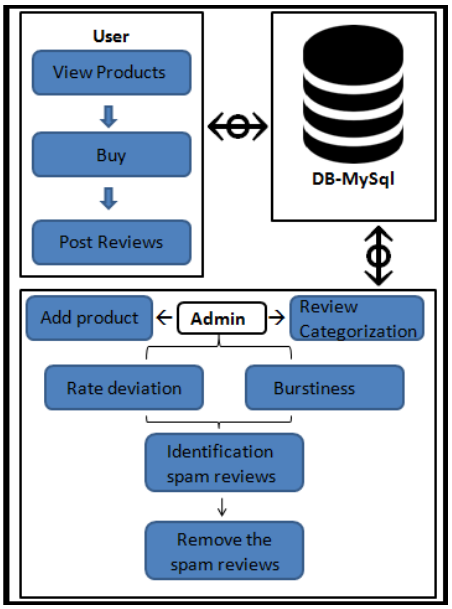

Figure 1. Proposed System Architecture

The proposed framework includes two methodologies namely, Rate Deviation using Threshold and User Behavioral method for

identifying spammer and spam contents in an effective manner. In Rate Deviation using Threshold method, it calculates a score value against each user rating and overall rating of a product. Whereas in User Behavioral method, it calculates the user burst time. The above figure 3.1 represents architecture diagram of proposed system. It includes two users, admin and customers (users). The customer search for the products. The decision to buy / reject a product is based on analyzing the posted reviews. Once the customers are fully satisfied with the reviews (feedbacks), he / she will buy the product or else he / she won't buy the product. Finally, the customers who buy the products can able to post the review on the particular e-commerce site.

On the other hand, all e-commerce sites are managed by admin. For each admin, he / she has an individual login. Only an authorized admin can able to access / manage the site. The admin is responsible to add a product, delete a product, analysis the customer / user reviews there by identifying the spammers and spam content.

The detection of spammers and spam reviews is done by two methods:

1. Rate Deviation using Threshold
2. User Behavioral Method

Rate Deviation using Threshold

In this method, a score value is calculated against each user rating and overall user rating of a particular product. Here, the admin sets a threshold value say 0.5[1]. The generated score value compared with the threshold value. If the score value is lesser than the threshold value, then the admin detects that this review is a spam review which was posted by a spammer. Once the admin detects the spam review, he / she has an authority to remove the spam review from the site. The Score value is calculated using,

$$\text{Score} = 1 - \frac{(\text{user rate of item} - \text{average rate of item})}{4}$$

User Behavioral Method

Here, the behavior of individual user is analyzed by calculating user burst time. For each user given a product "p" which has a set of "m" reviews posted by same user $\{p_1, \ldots, p_m\}$, and each review has a review date associated with it $\{t_1, \ldots, t_m\}$. So, the duration of each product review is computed by $t_m - t_1$ which is considered as the difference between the latest review date and the first review date.

Here the life span of the product is divided into small sub-intervals or bins by choosing a proper bin size. In this paper, we set bin value as 28 days. Then we compute the average number of reviews within each bin as follows ,

$$\text{Score} = 1 - \frac{(\text{Last review date of the product } (t_m) - \text{First review date of the product } (t_1))}{28}$$

The Calculated score value is again compared with the threshold value (say 0.5) set by the admin. If the score value is greater than the threshold value, then the admin detects that this review is a spam review which was posted by a spammer [5]. Once the admin detects the spam review, he / she has an authority to remove the spam review from the site.

III. CONCLUSION

The main challenging problem faced by the companies nowadays is detecting and eliminating spammer and spam reviews from the e-commerce sites. The positive or negative spam reviews may mislead the user / customer in purchasing a product. On the other side, it may improve the profit of a company or reduce the reputation of a company. In our proposed system the spammer and spam review is detect by two methodologies namely, Rate Deviation using Threshold and User Behavioral method for identifying spammer and spam contents in an effective manner. In Rate Deviation using Threshold method, it calculates a score value against each user rating and overall rating of a product. Whereas in User Behavioral method, it calculates the user burst time.

IV. REFERENCES

[1]. Prof Saeedreza Shehnepoor, Mostafa Salehi, Reza Farahbakhsh, Noel Crespi, NetSpam: a Network-based Spam Detection Framework for Reviews in Online Social Media, 2017.

[2]. A. j. Minnich, N. Chavoshi, A. Mueen, S. Luan, and M. Faloutsos. Trueview,Harnessing the power of multiple review sites.2015.

[3]. B. Viswanath, M. Ahmad Bashir, M. Crovella, S. Guah, K. P. Gummadi, B. Krishnamurthy, and A. Mislove.Towards detecting anomalous user behavior in online social networks. ,2014.

[4]. H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao.,Spotting fake reviews via collective PU learning,2014.

[5]. Geli Fei, Arjun Mukherjee , Bing Liu , Meichun Hsu, Malu Castellanos, Riddhiman Ghosh . Exploiting Burstiness in Reviews for Review Spammer Detection, 2015

[6]. Satish Tukaram Pokharkar, Ajit Jaysingrao Shete, Vishal Dyandeo Ghogare,Survey in Online social media Skelton by network based spam,2017

[7]. Snehal Dixit1 & A.J.Agrawal,Survey on Review Spam Detection, 2013.

[8]. Kolli Shivagangadhar, Sagar H, Sohan Sathyan, Vanipriya C.H,Fraud Detection in Online Reviews using Machine Learning Techniques, 2015

[9]. Sunita Mahajan1, Dr. Vijay Rana ,Spam Detection on Social Network through Sentiment Analysis,2017

[10]. Sushant Kokate, Bharat Tidke ,Fake Review and Brand Spam Detection using J48 Classifier ,2015

[11]. Siddu P. Algur, Jyoti G. Biradar ,Opinion Mining and Review Spam Detection: Issues and Challenges ,2017

[12]. Ahmed Abu Hammad ,Alaa El-Halees ,An Approach for Detecting Spam in Arabic Opinion Reviews,2015