IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 3, June 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Detection of Spammer Group Using Semi-Supervised Learning

[1] Bindhya Babu; [2] Sam G Benjamin

[1] CSE DEPARTMENT, BMCE
APJ Abdul Kalam Technological University, Sasthamcotta, Kerala, India

[2] CSE DEPARTMENT, BMCE
APJ Abdul Kalam Technological University, Sasthamcotta, Kerala, India

Abstract: These days, online items survey assumes a pivotal job for purchasing online products. A high extent of positive surveys will bring considerable deals development while negative surveys will cause deals misfortune. Driven by huge money related benefits, various spammers attempt to advance their items or downgrade their rivals' items by posting fake and one-sided online surveys. Existing works extract spammer candidates and remove spammers from the review data using unsupervised spamicity positioning techniques. All things considered, as indicated by past research, marking few spammer group is simpler than one expect, number of techniques endeavor to utilize significant named information. In this paper, we propose a semi-supervised learning technique to distinguish spammers. Naive Bayesian model and EM calculations are used to organize a classifier for the detection of spammer groups.

Keywords: *Naive Bayesian Model, EM Calculations, Spammer Groups, Semi-Supervised Learning.*

1. Introduction

E-commerce online item reviews become increasingly more significant as the purchase choices of the customers are strongly affected by these reviews. Because of the financial budgetary many spammers attempt to write fake reviews to advance their items or downgrade their rivals' items. These spammer teams either called review spammers or opinion spammers. As there are numerous accounts, the spammers could take total management of the sentiment on their objective items with little anomalous behaviour. As there are generally no labelled instances groups, most existing work discover spammer team candidates first and afterwards unsupervised learning techniques are used to recognize genuine spammers from these candidates. As per the research we could easily name (label) a few groups manually to acquire some named labelled instances. It is clear that combination of labelled instances and other unlabeled groups will altogether improve the precision of spammer team discovery.

This paper proposes a technique to recognize spammer teams, since commentators in the group write reviews on different items, the data mining technique frequent item set mining can be utilized to discover them. However, so found groups are just group spam candidates because numerous groups might be fortuitous, as certain reviewers happen to review a similar set of items because of comparable tastes and ubiquity of the items. Therefore, our focus is to distinguish genuine spammer groups from the candidate set.

Secondly, accessing those utilizing criteria that show a typical behaviour of groups, finally use semi supervised learning such as Naive bayes classifier and Expectation Maximization to find spammers. The experiment depends on a large set of Amazon reviewers and their surveys.

2. Related Works

Detecting Spammer Groups from Product Reviews, A Partially Supervised Learning Model by Lu Zhang et al., [1]. They propose a partially supervised learning model to identify spammer groups. By naming (labeling) some spammer groups as positive occurrences; PSGD applies Positive Unlabeled Learning (PU-Learning) to study a classifier as spammer group identifier from positive instances (named spammer groups) and unlabeled instances (unlabeled gatherings). They select reliable negative set in terms of the positive instances and the distinctive highlights. By consolidating the positive instances, extracted negative instances and unlabeled instances, it convert the PU-Learning issue into the outstanding semi-supervised learning issue, and afterward utilize Naive Bayesian model and EM calculation to prepare a classifier for spammer group detection.

Detecting group review spam by Arjun Mukherjee et al., [2]. They propose a method of identifying such groups comprises pattern mining to find spammer groups evaluating candidates using criteria indicating atypical group behaviours and finally ranking candidate groups.

Detection of Fake Review and Brand Spam Using Data Mining Technique by Miss.Rashmi Gomatesh Adike et al., [3]. They propose a technique to identifying the untruthful reviews that are given by the clients contains distinct semantic content dependent on sentimental analysis. For classifying they use j48 classifier and produce ARFF (Attribute-Relation File Format) from the distinct features to identifying the untruthful surveys. Utilizing support count in association rules they further identify brands in fake reviews.

Spotting Fake Reviewer Groups in Consumer Reviews by Arjun Mukherjee et al., [4]. The recommended methodology initial utilize pattern mining to seek out a set of applicant groups, from that a labeled set of spammer team was created. Though labeling individual fake audits or commentors is tough, labeling groups is significantly easier. In order that they recommend many behavior features derived from collusion among fake commentors. A unique relation-based model gsrank was bestowed which might take into account relationships among groups individual commentors and product they analyzed to find spammers.

3. Proposed System

A spammer group consists of a collection of reviewers who co-reviews a set of common product. Thus, the data mining technique Frequent Itemset Mining (FIM) could be used to extract the groups. However, since many users could also be coincidently grouped due to the similar interest, the groups extracted by FIM are solely the spammer group candidates and need to be further checked to identify the real spammer groups. Our proposed methodology works in 3 stages:

Stage 1 - Find candidate groups using pattern mining:

In this stage we extract review data to provide a lot of transactions. Every transaction represents a novel item and comprises all reviewers (their ids) who have looked into that item. Utilizing every transaction we can perform mining for subsequent patterns. The subsequent itemset are spammer groups.

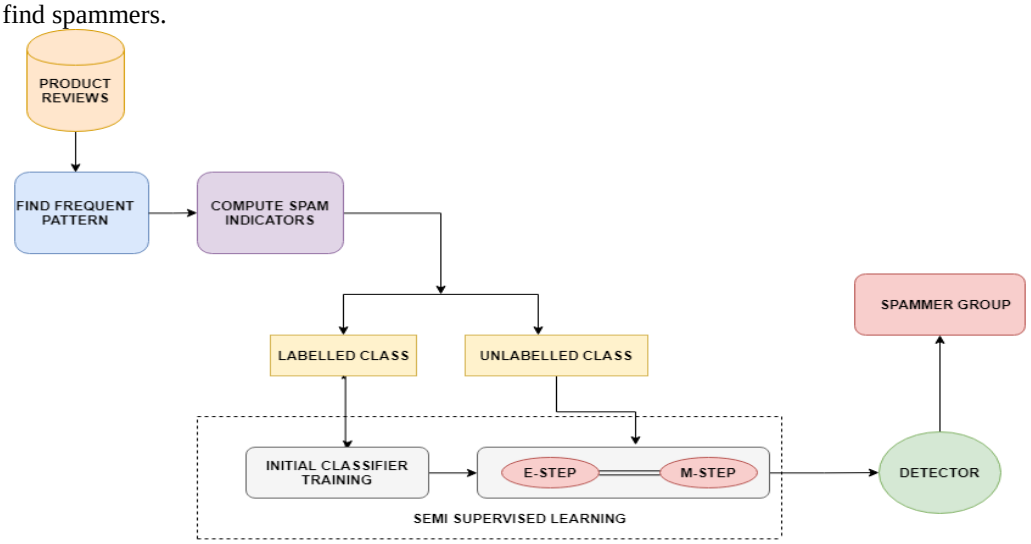

Fig 1: Overview of the proposed system

Stage 2 - Computing Spam Indicator Values: Many of the candidate groups may not be genuine spammer groups. This stage endeavors to assess them dependent on a set of abnormal behaviors to see if these groups behave strangely. 8 criteria are designed.

Group Time Window (GTW): Individuals in a spam groups are probably cooperated together in posting reviews for particular products during a short span interval.

Group Deviation (GD): A highly harming spam group happens when the ratings of individuals in the group deviate a lot from those of other commentators to change the sentient on an item. The bigger the deviation, the worse the group is.

Group Content Similarity (GCS): Group connivance is additionally exhibited by content similarity once. Spammers copy reviews among themselves. So the misused items have several audits with similar content.

Group Member Content Similarity (GMCS): The members of a gaggle might not recognize one another. Each of them simply copy or modify their own previous reviews. If multiple members of the cluster (group) try this the cluster is more probably to be a spammer group.

Group Early Time Frame (GETF): Reports spammers typically review early to create the largest impact. Similarly once group members are the initial people to review a product they can completely hijack the emotions on the products.

Group Size Ratio (GSR): The proportion of group size to total range of commentators for an item can indicate spamming. Assuming the worst possible scenario, the group members are the main commentators of the item totally controlling the sentiment on the item. Then again, if the total range of commentators of the item is vast, then the impact of the group is little.

Group Size (GS): Group collusion is also exhibited by its size. For big groups chance of members happening to be along is little. Moreover the larger the group is a lot of damaging it's.

Group Support Count (GSUP): Support count is the number of products that the group has worked together. If any group encompasses high support count its clearly terrible.

Stage 3 - Train utilizing semi-supervised learning: 2 classes will be obtained after the extraction of spam indicator values. Labeled category contains with certifiable and fake reviews though unlabeled category incorporates with the rest of spammer gather candidates with obscure classes. Based on category labeled and unlabeled, a semi-supervised learning classifier is prepared to recognize genuine spammer groups, initial train a Naive Bayes classifier on labeled set, then incorporate unlabeled information set with Expectation Maximization (EM) algorithmic rule to boost initial classifier. During this procedure, labeled occurrences are utilized to decide the parameters of probability distribution of each category. To exploit, the unlabeled information, we tend to utilize the Expectation Maximization (EM) algorithmic rule, a wide utilized approach that interactively re-estimates parameters by repeating the 2 sorts of steps (E-Step and M-Step) till the parameters' meeting to stationary values.

4. Experimental Result

The research is conducted utilizing substantial number of analysts and audits of manufactured items from Amazon.com. The comparison results exhibit to acquire high performance, the supervised learning require a lot of labeled instances to prepare the classifier, in any case, as including the unnamed instances, the semi – supervised learning needs less named instances and only positive instances.

Table 1: Comparison Between Methods

Classifiers	Accuracy
Naive Bayes And Expectation Maximization	94%
Logistic Regression	84.6%
Random Forest	69%
Support Vector Machines	88%

5. Conclusion

As individuals and businesses are progressively utilizing surveys for their choices making, it is critical to distinguish spammers who write counterfeit surveys. This paper proposed a successful strategy to distinguish spammer groups who cooperate to write counterfeit surveys. First, the PSGD model uses frequent item mining (FIM) to discover spammer group candidates from the review data. Then, by manually labeling some spammer groups as positive instances, the PSGD employs PU-Learning to construct a classifier from the positive and unlabeled instances to identify the real spammer groups from group candidates.

References

[1] Detecting Spammer Groups from Product Reviews: A Partially Supervised Learning Model by LU ZHANG, ZHIANG WU, (MEMBER, IEEE), AND JIE CAO, 10.1109/ACCESS.2017.2784370, IEEE Access

[2] Detecting Group Review Spam by Arjun Mukherjee, Bing Liu, Junhui Wang, Natalie Glance, Nitin Jindal, Dept of CS. Technical Report, UIC, 2011.

[3] Detection of Fake Review and Brand Spam Using Data Mining Technique by Miss.Rashmi Gomatesh Adike, Prof. Vivekanand Reddy, Volume 02, Issue 07; July - 2016 [ISSN: 2455-1457]

[4] H. Li, B. Liu, A. Mukherjee, and Natalie Glance, "Spotting fake reviewer groups in consumer reviews," Computación y Sistemas, vol. 18, no. 3, pp. 467–475, 2014.

[5] L. Akoglu, R. Chandy, and C. Faloutsos, "Opinion fraud detection in online reviews by network effects." ICWSM, vol. 13, pp. 2–11, 2013.

Author Profile

Bindhya Babu received her B. Tech (CSE) degree from University of Kerala in 2017. She is currently pursuing her Masters in Computer Science & Engineering from KTU.

Sam G Benjamin is working as Assistant Professor in Computer Science and Engineering Department. His research interests focuses on image processing, data mining and image mining. He has published papers on image processing.