Spam Review and services on Social Sites using Heterogeneous Information Network

Syed Arifa[1], Dr. D. N. V. Syam Kumar.[2]

[1] M.Tech Research Scholar, St. Ann's College of Engineering & Technology, Chirala.

[2] Associate professor & Research Supervisor, St. Ann's College of Engineering & Technology, Chirala

arifasyed7861@gmail.com, sacetfaculty.syam@gmail.com

ABSTRACT

Today's, a major part of everyone trusts on content in social media like opinions and feedbacks of a topic or a product. The liability that anyone can take off a survey give a brilliant chance to spammers to compose spam surveys about products and services for various interests. Recognizing these spammers and the spam content is a wildly debated issue of research and in spite of the fact that an impressive number of studies have been done as of late toward this end, yet so far the procedures set forth still scarcely distinguish spam reviews, and none of them demonstrate the significance of each extracted feature type. In this investigation, we propose a novel structure, named Net Spam, which uses spam highlights for demonstrating review datasets as heterogeneous information networks to design spam detection method into a classification issue in such networks.

Utilizing the significance of spam features help we to acquire better outcomes regarding different metrics on review datasets. The outcomes demonstrate that Net Spam results the existing methods and among four categories of features; including review-behavioral, user-behavioral, review linguistic, user-linguistic, the first type of features performs better than the other categories. The contribution work is when user search query it will display all top-k products as well as recommendation of the product.

INTRODUCTION

1.1 Introduction

Online Social Media portals play an influential role in information propagation which is considered as an important source for producers in their advertising campaigns as well as for customers in selecting products and services. In the past years, people rely a lot on the written reviews in their decision-making processes, and positive/negative reviews encouraging/discouraging them in their selection of products and services. In addition, written reviews also help service providers to enhance the quality of their products and services. These reviews thus have become an important factor in successor a business while positive reviews can bring benefits for accompany, negative reviews can potentially impact credibility and cause

economic losses. The fact that anyone with any identity can leave comments as review provides a tempting opportunity for spammers to write fake reviews designed to mislead users' opinion. These misleading reviews are then multiplied by the sharing function of social media and propagation over the web. The reviews written to change users 'perception of how good a product or a service are considered as spam[11] and are often written in exchange for money 20% of the reviews in the Yelp website are actually spam reviews. On the other hand, a considerable amount of literature has-been published on the techniques used to identify spam and spammers as well as different type of analysis on this topic. These techniques can be classified into different categories; some using linguistic patterns in text which are mostly based on bigram, and unigram, others are based on behavioural patterns that rely on features extracted from patterns in users' behaviour which are mostly metadata based [6],[9]and even some techniques using graphs and graph-based algorithms and classifiers.

Despite this great deal of efforts, many aspects have been missed or remained unsolved. One of them is a classifier that can calculate feature weights that show each feature's level of importance in determining spam reviews. The general concept of our proposed framework is to model a given review datasets a Heterogeneous Information Network (HIN) and to map the problem of spam detection into a HIN classification problem. In particular, we model review dataset as a HIN in which reviews are connected through different node types (such as features and users). A weighting algorithm is then employed to calculate each feature's importance (or weight).

These weights are utilized to calculate the final labels force views using both unsupervised and supervised approaches. To evaluate the proposed solution, we used two sample review datasets from Yelp and Amazon websites. Based on our observations, defining two views for features (review-user and behavioural-linguistic), the classified features as review behavioural have more weights and yield better performance on spotting spam reviews in both semi-supervised and unsupervised approaches. In addition, we demonstrate that using different supervisions such as 1%, 2.5% and 5% or using an unsupervised approach, make no noticeable variation on the performance of our approach. We observed that feature weights can be added or removed for labelling and hence time complexity can be scaled for a specific level of accuracy. As the result of this weighting step, we can use fewer features with more weights to obtain better accuracy with less time complexity. In addition, categorizing features in four major categories (review-behavioural, user-behavioural, review linguistic, user-linguistic), helps us to understand how much each category of features is contributed to spam detection. In summary, our main contributions are as follows:(I) We propose Net Spam framework that is a novel network based approach which models review networks as heterogeneous information networks. The classification step uses different met path types which are innovative in the spam detection domain.(ii) A new weighting method

for spam features is proposed to determine the relative importance of each feature and shows how effective each of features are in identifying spasm from normal reviews. Previous works also aimed to address the importance of features mainly in term of obtained accuracy, but not as a build-in function in their framework (i.e., their approach is dependent to ground truth for determining each feature importance). As we explain in our unsupervised approach, Net Spam is able to find features importance even without ground truth and only by relying on met a path definition and based on values calculated for each review.

(iii) Net Spam improves the accuracy compared to the state of-the art in terms of time complexity, which highly depends to the number of features used to identify a spam review; hence, using features with more weights will resulted in detecting fake reviews easier with less time complexity.

II. Existing System

- Existing system techniques can be classified into different categories; some using linguistic patterns in text which are mostly based on bigram, and unigram, others are based on behavioral patterns that rely on features extracted from patterns in users' behavior which are mostly meta data based and even some techniques using graphs and graph-based algorithms and classifiers.
- Existing system can be summarized into three categories: Linguistic-based Methods, Behavior-based Methods and Graph-based Methods.
- Fang et al. use unigram, bigram and their composition. Other studies use other features like pair wise features (features between two reviews; e.g. content similarity), percentage of CAPITAL words in reviews for finding spam reviews.
- Lai et al. used a probabilistic language modeling to spot spam. This study demonstrates that 2% of reviews written on business websites are actually spam.
- Deeper analysis on literature show that behavioral features work better than linguistic ones in term of accuracy they yield.

2.1 Disadvantages

- The fact that anyone with any identity can leave comments as review provides a tempting opportunity for spammers to write fake reviews designed to mislead users' opinion. These misleading reviews are then multiplied by the sharing function of social media and propagation over the web.
- Many aspects have been missed or remained unsolved.
- Previous works also aimed to address the importance of features mainly in term of obtained accuracy, but not as a build-in function in their framework (i.e., their approach is dependent to ground truth for determining each feature importance).

III. Proposed system:

- The general concept of our proposed framework is to model a given review dataset as a Heterogeneous Information Network (HIN) and to map the problem of spam detection into a HIN classification problem.
- In particular, we model review dataset as a HIN in which reviews are connected through different node types (such as features and users). A weighting algorithm is then employed to calculate each feature's importance (or weight). These weights are utilized to calculate the final labels for reviews using both unsupervised and supervised approaches.
- We propose Net Spam framework that is a novel network based approach which models review networks as heterogeneous information networks. The classification step uses different met path types which are innovative in the spam detection domain.
- A new weighting method for spam features is proposed to determine the relative importance of each feature and shows how effective each of features are in identifying Spasm from normal reviews.
- Net Spam improves the accuracy compared to the state of- the art in terms of time complexity, which highly depends to the number of features used to identify a spam review; hence, using features with more weights will resulted in detecting fake reviews easier with less time complexity.

3.1 Advantages

- Improved Accuracy
- Easier in detecting fake reviews
- Less time Complexity
- As we explain in our UN supervised approach, Net Spam is able to find features importance even without ground truth, and only by relying on Meta path definition and based on values calculated for each review.
- There are no previous methods which engage importance of features (known as weights in our proposed framework; Net Spam) in the classification step. By using these weights, on one hand we involve features importance in calculating final labels and hence accuracy of Net Spam increases, gradually.
- On the other hand we can determine which feature can provide better performance in term of their involvement in connecting spam reviews (in proposed network).

IV. NETSPAM ALGORITHM

Aim of the proposed algorithm is to detect the spam reviews on online social media by giving weight age to the features which are extracted. The proposed algorithm consists of four main steps.

Step 1: Prior Knowledge:

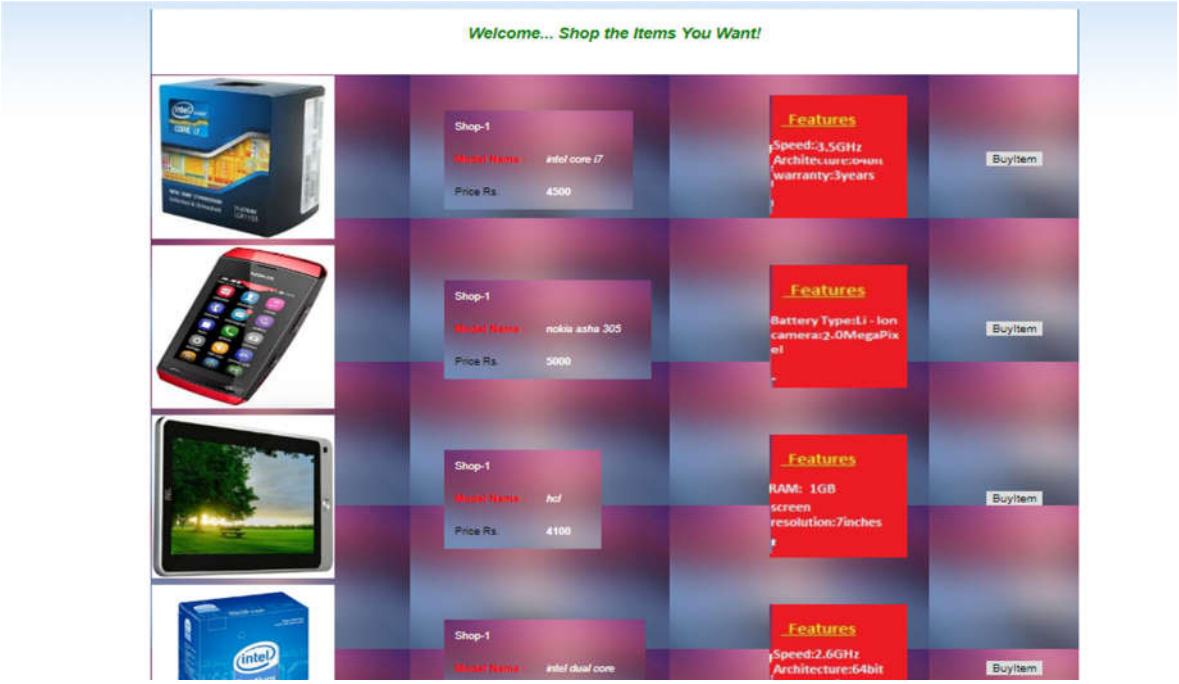
The initial step is processing earlier learning, i.e. the underlying likelihood of survey u being spam which signified as the proposed structure works in two forms; semi-supervised learning and unsupervised learning. In the semi supervised technique, if review u is named as spam in the pre-named reviews, generally. On the off chance that the mark of this audit is obscure due the measure of supervision, consider (i.e., accept u as a non-spam survey). In the unsupervised technique, our earlier information is acknowledged by utilizing the likelihood of survey u being spam as indicated by feature and L is the quantity of all the utilized highlights.

Step 2: Network Schema Definition:

Thenextstepisdeningnetworkschemabasedonagivenlistofspamfeatureswhich decides the highlights occupied with spam discovery. This Schema is general definitions of met paths and show when all is said in done how unique system segments are associated. Step 3: Met path definition and creation: A met path is defined by a grouping of relations in the system schema. For met path creation, defined a broadened rendition of the met path idea considering diverse levels of spam certainty. In particular, two reviews are connected to each other if they share same esteem. Hassanzadeh et al. propose a fluffy based structure and show for spam recognition; it is smarter to utilize fluffy rationale for deciding an audits name as a spam or non-spam. Surely, there are diverse levels of spam assurance. Utilized a stage capacity to decide these levels. Specifically, given a review u, the levels of spam conviction for met path (i.e., highlight l) are ascertained as where s signifies the number of levels. After computing for all reviews and met paths, two reviews and v with the same met path esteems for met path are associated with each other through that met path and make one connection of survey organize. The met path esteem between them indicated as. Using s with a higher esteem will build the quantity of every component met paths high and here consequently fewer reviews would be associated with each other through these highlights. Then again, utilizing lower an incentive for s drives us to have bipolar esteems (which implies surveys take esteem 0 or 1). Since require enough spam and non-spam audits for each progression, with less number of surveys associated with each other for each progression, the spam likelihood of surveys take uniform circulation, yet with bring down estimation of s have enough reviews to ascertain all spam city for each reviews. In this manner, precision for bring down levels of s diminishes on account of the bipolar issue, and it decades for higher estimations of s, since they take uniform circulation. Step 4: Classification: The classication step of Net Spam contains twosteps ;(i)weightcalculationwhichdeterminestheimportanceofeachspamfeaturein determining spam reviews, (ii)labeling which computes the final likelihood of each survey being spam. At next we depict them in detail. 1. Weight Calculation: This progression registers the heaviness of each met path. Expect that nodes classification is done in terms of their relations to different nodes in the review arrange; connected nodes may have a high likelihood of taking similar names. The relations in a heterogeneous data arrange incorporate the immediate connection as well as the way that can be estimated by utilizing the met path idea. Consequently, need to use the met paths denned in the past advance, which represent theater ogeneousrelationsamongnodes. Moreover,thisstepwill have the capacity to register the heaviness of every connection way (i.e., the significance of the met path), which will be utilized as a part of the following stage (Labeling) to appraise the name of each unlabeled review. The weights of the met paths will answer an important question; which met path (i.e., spam highlight) is better at positioning spam audits Also, the weights help us to comprehend the development system of a spam survey. What's more, since some of

these spam highlights may in cur consider able computational costs(for example, computing linguistic-based highlights through NLP strategies in a huge audit dataset), picking the more significant highlights in the spam discovery methodology prompts better execution whenever the computation cost is an issue. To compute the weight of met path p□ore = 1, …,L where L is the quantity of met paths, Here propose condition :

V. SCREEN SHOTOS



VI CONCLUSION

This study introduces a novel spam detection framework namely Net Spam based on a meta path concept as well as a new graph-based method to label reviews relying on a rank-based labeling approach. The performance of the proposed framework is evaluated by using two real-world labelled datasets of Yelp and Amazon websites. Our observations show that calculated weights by using this meta path concept can be very effective in identifying spam reviews and leads to a better performance. In addition, we found that even without a train set, Net Spam can calculate the importance of each feature and it yields better performance in the features' addition process, and performs better than previous works, with only a small number of features.

Moreover, after defining four main categories for features our observations show that the reviews behavioural category performs better than other categories, in terms of average precision(AP) and are under the curve(AUC) as well as in the calculated weights. The results also confirm that using different supervisions, similar to the semi-supervised method, have no noticeable effect on determining most of the weighted features, just as in different datasets. For future work, meta path concept can be applied to other problems in this field. For example, similar framework can be used to find spammer communities. For finding community ,reviews can be connected through group spammer features and reviews with highest similarity based on meta path concept are known as communities. In addition, utilizing the product features is an interesting future work on this study as we used features more related

to spotting spammers and spam reviews. Moreover, while single networks has received considerable attention from various disciplines for over a decade, information diffusion and content sharing in multilayer networks is still a young research. Addressing the problem of spam detection in such networks can be considered as a new research line in this field.

VII FUTURE ENHANCEMENT

Here in this project for the future scope we can use some encryption technique while the data is transferred for the security purpose. Initially the data is encrypted while transferring the data to the node but if the node fails then the application will encrypt using the other algorithm and then the alternate path will be chose and accordingly the data will be transferred

VIII REFERENCES

[1]. J. Donfro, A whopping 20 % of yelp reviews are fake. http://www.businessinsider.com/20-percent-of-yelpreviews-fake-2013-9. Accessed: 2015-07-30.

[2]. M. Ott, C. Cardie, and J. T. Hancock. Estimating the prevalence of deception in online review communities. In ACM WWW, 2012.

[3]. M. Ott, Y. Choi, C. Cardie, and J. T. Hancock. Finding deceptive opinion spam by any stretch of the imagination.In ACL, 2011.

[4]. Ch. Xu and J. Zhang. Combating product review spam campaigns via multiple heterogeneous pairwise features. In SIAM International Confer-ence on Data Mining, 2014.

[5]. N. Jindal and B. Liu. Opinion spam and analysis. In WSDM, 2008.

[6]. F. Li, M. Huang, Y. Yang, and X. Zhu. Learning to identify review spam. Proceedings of the 22nd International Joint Conference on Artificial Intelligence; IJCAI, 2011.

[7]. G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh. Ex-ploiting burstiness in reviews for review spammer detection. In ICWSM, 2013.

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

[9]. 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. In USENIX, 2014.

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

[11]. L. Akoglu, R. Chandy, and C. Faloutsos. Opinion fraud detection in online reviews bynetwork effects. In ICWSM, 2013.

AUTHOR DETAILS:

Syed.Arifa received B.Tech from St.Ann's Engineering College in 2016. Currently Pursuing M. Tech in Computer Science and Engineering at St.Ann's College of Engineering & Technology which is affiliated under JNTU Kakinada. My area of interests are Programming languages and Computer Security.

D.N.V. Syam Kumar presently working as an Associate Professor in the department of computer science & engineering at St.Anns College of Engineering &

Technolgy, Chirala. He was received his Ph.d degree from Krishna University in the stream of Computer Science & Engineering. He was guided so many UG & PG projects. He worked in many well known engineering colleges of Andhra pradesh and also worked as Head of the department of CSE. He was published 10 international journals. He was attended so many technical seminars, national and international conferences all over the india. He was having 15 years of professional experience. His research interests are software engineering, testing and image processing. He can be contacted on 9963055788 & email – sacetfaculty.syam@gmail.com