Journal of Engineering Sciences

Vol 10, Issue 11 , Nov /2019
ISSN NO:0377-9254

A STUDY ON THE FRAMEWORKS OF WEB SPAM DETECTION USING HETEROGENEOUS DATA SETS

D.SURENDRA[1], K SAIKIRAN[2],G.PRUDHVI[3], K SAITEJA[4]

Assistant Professor[1], UG Student[234]

Dept of CSE, ASCET, Gudur

ABSTRACT

In recent days, many people rely on available content in social media in their decisions for referring feedback on products. The possibility that anybody can leave a review provides a golden opportunity for spammers to write spam reviews about products and services for different interests. Identifying these spammers and the spam content is a hot topic of research and although a considerable number of studies have been done recently toward this end, but so far the methodologies put forth still barely detect spam reviews, and none of them show the importance of each extracted feature type. In this study, propose a novel framework, named WebSpam, which utilizes spam features for modeling review datasets as heterogeneous information networks to map spam detection procedure into a classification problem in such networks. Using the importance of spam features helps to obtain better results in terms of different metrics experimented on real-world review datasets from Yelp and Amazon websites. The results show that WebSpam outperforms the existing methods and among four categories of features.

Keywords: WebSpam, Heterogeneous Information Network, spam features, Social media, User-linguistic.

I.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 the success of a business while positive reviews can bring benefits for a company, 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 the user's opinion. These misleading reviews are then multiplied by the sharing function of social media and propagation over the web. The reviews written to change user's perception of how good a product or a service is considered as spam and are often written in exchange for money.

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, the 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. To evaluate the proposed solution, it used two-sample review datasets from Yelp and Amazon websites.

Based on the observations, defining two views for features (review-user and behavioral linguistic), the classified features as review behavioral have more weights and yield better performance on spotting spam reviews in both semi-supervised and unsupervised approaches. In addition, 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 the approach. The system observed that feature weights can be added or removed for labeling and hence time complexity can be scaled for a specific level of accuracy. As a result of this weighting step, it can use fewer features with more weights to obtain better accuracy with less time complexity. In addition,

categorizing features in four major categories (review-behavioral, user-behavioral, review linguistic, user-linguistic), helps us to understand how much each category of features is contributed to spam detection

II.RELATED WORKS

Model the problem as a heterogeneous network where nodes are either real components in a dataset (such as reviews, users, and products) or spam features. To better understand the proposed framework first presents an overview of some of the concepts and definitions in heterogeneous information networks.

Scott Clayton [4] proposed a new method to detect the spam by using Azure machine learning. Here Author trained classifiers in Azure to identify whether that message was spam or not. He used 16 bit hash for 65,536 features and selected best of the 1000. Author explored direct word frequency approach to get the accuracy; surprisingly author got 99 % accuracy in his article.

Paras sethi et.al [5] dealed with SMS spam detection and coma ping of different machine learning algorithms in their article. In every spam detection Bayesian filters will play a major role. Here authors compared different algorithms on spam detection by taking a public survey in mobile applications. They took two data sets for validation and testing purpose. The results gave different feature classification of spam messages under different algorithms.

Son dinh et.al [6] proposed a soft ware frame work for spam campaign detection, analysis and investigation. The frame work gives law enforcement administrators a platform to perform the investigation on the cyber crimes. By combining the spam mails into campaigns it minimizes the investigation efforts. To handle the huge number of spam mails they kept feature-rich and scalable database. The proposed frame work recognizes spam operations on fly. Adding to this it labels gathers the information and scores the campaigns.

Victor.M.Prieto et.al [7] proposed a content based web spam analyzer and detector in their article. They concentrated on www; means websites. Web spam is the major problem in today's world. This chapter deals with study of different types of web spam pages and detects the new elements in it to describe the heuristics capable to detect them. They proposed a new method called SAAD means spam analyzer and detector works based on C4.5 classifier improved by boosting and bagging methods. This one is also very effective in finding spam data sets.

III.EXISTING SYSTEM

Online Social Media websites play a main role in information propagation which is considered as an important source for producers in their advertising operations as well as for customers in selecting products and services. People mostly believe in the written reviews in their decision-making processes, and positive/negative reviews encouraging/discouraging them in their selection of products and services. These reviews thus have become an important factor in the success of a business while positive reviews can bring benefits for a company, negative reviews can potentially impact credibility and cause economic losses. The fact that anyone with any identity can leave comments as reviews provides a tempting opportunity for spammers to write fake reviews designed to mislead the user's opinion. These misleading reviews are then multiplied by the sharing function of social media and propagation over the web. The reviews written to change user's perception of how good a product or a service are considered as spam, and are often written in exchange for money.

IV.DEMERITS OF EXISTING SYSTEM

1. There is no information filtering concept in the online social network.

2. People believe in the written reviews in their decision-making processes, and positive/negative reviews encouraging/discouraging them in their selection of products and services.

3. Anyone create registration and gives comments as reviews for spammers to write fake reviews designed to misguide the user's opinion.

4. Less accuracy.

5. More time complexity.

V.PROPOSED SYSTEM

The 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, the 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. Based on the observations, defining two views for features (review-user and behavioral-linguistic), the classified features as review behavioral have more weights and yield better performance on spotting spam reviews in both semi-supervised and unsupervised approaches. The feature weights can be added or removed for labeling and hence time complexity can be scaled for a specific level of accuracy. Categorizing features in four major categories (review-behavioral, user-behavioral, review-linguistic, user-linguistic), helps us to understand how much each category of features is contributed to spam detection.

- Web spam framework is a novel network-based approach that models review networks as heterogeneous information networks.
- A new weighting method for spam features is proposed to determine the relative importance of each feature and shows how effective each of the features is in identifying spam from normal reviews.
- Web spam improves accuracy compared to state-of-the-art in terms of time complexity, which highly depends on the number of features used to identify a spam review.

VI.FEATURES OF THE SYSTEM

1. To identify spam and spammers as well as different types of analysis on this topic.

2. Written reviews also help service providers to enhance the quality of their products and services.

3. To identify the spam user using positive and negative reviews in online social media.

4. To display only trusted reviews to the users.

VII.CONCLUSION

This investigation presents a novel spam detection system, in particular, Web spam in view of a met path idea and another graph-based strategy to name reviews depending on a rank-based naming methodology. The execution of the proposed structure is assessed by utilizing review datasets. Our perceptions demonstrate that ascertained weights by utilizing this met path idea can be exceptionally powerful in recognizing spam surveys and prompts a superior execution. Furthermore, it found that even without a prepare set, NetSpam can figure the significance of each element and it yields better execution in the highlights' expansion procedure, and performs superior to anything past works, with just a few highlights. In addition, in the wake of characterizing four fundamental classifications for highlights our perceptions demonstrate that the review behavioral classification performs superior to anything different classifications, regarding AP, AUC and in the ascertained weights. The outcomes likewise affirm that utilizing diverse supervisions, like the semi-administered strategy, has no detectable impact on deciding the vast majority of the weighted highlights, similarly as in various datasets. Contribution part in this project, for the user, when searches query he will get the top-k hotel lists as well as one recommendation hotel by using personalized recommendation algorithm.

VIII. REFERENCES

1. Salma Farooq, Hilal Ahmad Khanday, "Opinion Spam Detection: A Review", International Journal of Engineering Research and Development (IJERD), Vol.12, No,4, pp no.1-8, 2016.

2. Nitin Jindal and Bing Liu ― Analyzing and Detecting Review Spam‖ in ICDM 2007 IEEE.

3. Hu and B. Liu. 2004. Mining and Summarizing Customer Reviews. In KDD, pages 168–177, Seattle, WA

4. Ana-Maria Popescu and Oren Etzioni ―Extracting Product Features and Opinions from Reviews ―.

5. Jindal, N., & Liu, B., "Identifying Comparative Sentences in Text Documents",SIGIR, 2006.

6. Ott, M., Cardie, C., & Hancock, J. T.,"Negative Deceptive Opinion Spam", In Proceedings of NAACLHLT, (pp. 497-501), 2013.

7. Ott, M., Cardie, C. and Hancock, J., "Estimating the Prevalence of Deception in Online Review Communities", Proceedings of the 21st international conference on World Wide Web, (WWW), 2012.

8. Ott, M., Choi, Y., Cardie, C. Hancock, J., "Finding Deceptive Opinion Spam by Any Stretch of the Imagination", Association of Computational Linguistics (ACL), 2011.

9. Yenuga Padma, Dr. Y.K Sundara Krishna, A Literature Review on Opinion Spam Detection and Its Approaches, International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 6, June 2017

10. 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.

11. SihongXie, 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.

12. MyleOtt, 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.

13. Ott, Myle, Claire Cardie, and Jeffrey T. Hancock. "Negative deceptive opinion spam." Proceedings of NAACL-HLT. 2013.

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

15. Li, F.; Huang, M.; Yang, Y.; and Zhu, X. 2011. Learning to Identify Review Spam. In IJCAI.

16. Lim, E.-P.; Nguyen, V.-A.; Jindal, N.; Liu, B.; and Lauw, H. W. 2010. Detecting product review spammers using rating behaviors.In CIKM, 939–948.

17. Mukherjee, A.; Liu, B.; and Glance, N. S. 2012. Spotting fake reviewer groups in consumer revies.

18. 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.

19. Uncovering social spammers: social honey pots and machine learning by kyumin lee, James caver lee and Steve webb, https://dl.acm.org/citation.cfm?id=1835522

20. Proposed efficient algorithm to filter spam using machine learning techniques by Ali Shafiguh aski, Navid k Sourati Pacific Science Review A: Natural Science and Engineering Volume 18, Issue 2, July 2016, Pages 145-149

21. Performance Evaluation of Machine Learning Algorithms for Spam Profile Detection on Twitter Using WEKA and RapidMiner by Hanif, Mohamad Hazim Md; Adewole, Kayode Sakariyah; Anuar, Nor Badrul; Kamsin, Amirrudin Source: Advanced Science Letters, Volume 24, Number 2, February 2018, pp. 1043-1046(4)

22. Detecting Spam with Azure Machine Learning by Scott Clayton, 12 Feb 2018.

23. SMS spam detection and comparison of various machine learning algorithms by Paras sethi et.al https://ieeexplore.ieee.org/document/8284445/

24. Spam campaign detection, analysis, and investigation by son dinh et.al https://www.sciencedirect.com/science/article/pii/S1742287615000079

25. SAAD, content based Web Spam Analyzer and Detector by Victor.M. Prieto et.al https://www.sciencedirect.com/science/article/pii/S0164121213001684.