ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

Automated Detection of Spambots in Social Media

Mrs.Yamini Priya V[1] ,Latha S [2] , Pavithra Devi S [3] , Lavanya S[4], Lakshmi K [5],

[1]Assistant Professor, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India

[2][3][4][5]Final Year, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India

ABSTRACT: Nowadays usage of social media is increasing. Most of the people depend on social media. Spammers use social media as a platform to leave their spam reviews about products and services. The open nature of social media and also the large number of user encourage the spammers to indulge in cyber crime, phishing, sending malicious links. Existing work depend on the reviews and spammers. Importance of each feature type is not taken into account. The technique can be classified into different types such as: linguistic pattern based on bigram, unigram, behavioral pattern rely on users behavior. In proposed approach the classification step uses different meta path which are innovative in spam detection. It shows how effective each of features in identifying spam from normal user and also improves the accuracy. The features with more weights will resulted in detecting fake reviews easier with less time complexity. This approach is more effective in identifying in spam review. It increases performance, the importance of spam features help us to obtain better results in terms of different metrics.

KEYWORDS: Social network, Spam detection, Bayesian network, spam reviews, Meta path.

I. INTRODUCTION

Social media play a vital role in sharing information to the society.OSN(Online Social Network) is a large user base and it attracts the people from various age groups.OSN makes use of people to always be in contact with everyone such as their friends, relatives they are far away.

Social media allows user to interact with each other and it helps to form some community. Any user can join as a member by providing some common details about them such as email id, mobile number, gender, date of birth and other information. In world wide Face book, Twitter are one among the top10 web sites. OSN change the normal social life. Increasing users are the major reason reasons for enlargement, data distribution, marketing, economic and

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

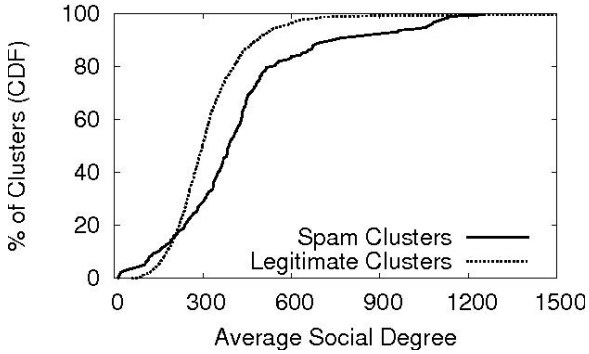
Vol. 8, Issue 3, March 2019

commerce. To fine our old friends social media is used. If there is a need of micro blogging Twitter is used. Linked in is one of the best media to preserve professional resume with high quality of contacts. Face book is the most visited social media it has 800 million network with 250 million guest per month. Most of the spammers try to focus on retrieving user information without any permission for advertising their products and services and also edition their posts on social media sites.

Using some methods spam reviews are detected at the starting stage by using user based and review based spammers are detected and alert will be given to the user.

II. PROBLEM STATEMENT

In existing they use Linguistic based, behavior based and graph based models. The linguistic based is used to find the spam reviews[1]. It uses unigram, bigram model. It identifies the percentage of capital words in reviews. In behavior base meta data to identify the pattern of the reviewer[3].



It uses the trust model to find relationship between users and to find usual behavior of spammer. To improve the performance they use some new features which has high complexity. In graph based model the aim is to draw graph between user review and spam review so, the reviews given by spammers are hard to find[4].

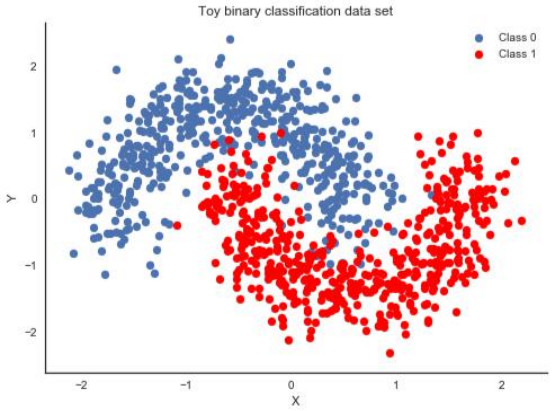
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

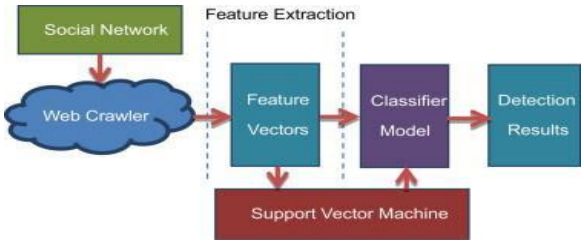
Vol. 8, Issue 3, March 2019



Generally spammers will hide their information[6]. In fact we add lot of features which will be high time consuming.

III. PROPOSED SYSTEM

We proposed net spam framework that is novel based approach which models review networks as heterogeneous information network. The classification step uses different meta path types which are efficient in the spam detection domain. In our proposed system to determine the relative importance of each feature and show how effective each of features are in identifying spam from normal reviews and also improves the accuracy. A weighting scheme is used to determine each features and also in identifying spam from normal reviews.



Net spam improves the accuracy compared to the state of the art in terms of time complexity, which highly depends on number of features used to identify spam review hence using features with more weights will result in detecting fake reviews with less time complexity.

IV. PREPROCESSING

In this module, collection of data from user is given as input to the system. Preprocessor process the data and remove unwanted words, blank space and symbols.

Meta path identification

This deals with analysis of various websites for identification of fake reviews. It shows the relation in network schema. It shows the different level of spam certainty. For that it need both spam and non spam reviews. The spam probability of review is taken as uniform distribution.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

Naïve Bayes

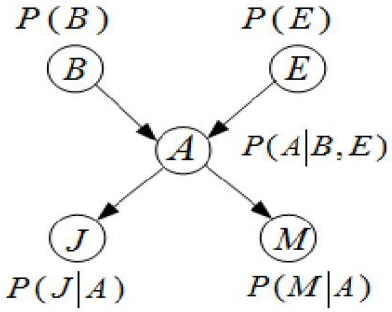
It is the statistical technique for spam filtering. It is based on posterior probability. Detection of spam is calculated based on review and if the probability value exceed the threshold then it is marked as spam.

Conflict detection

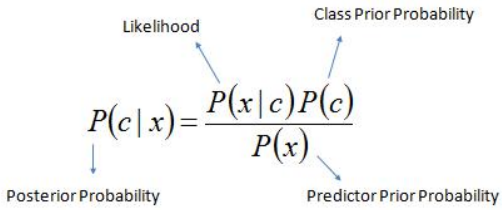
Classification makes the filtering detection before integration. If the message is notified as spam, it is clustered separately, and non spams are clustered separately.

Bayesian Theorem

Bayesian Theorem used to calculate posterior probability. P(c|x),p(c),p(x),p(x|c). Naive Bayes assume that value of predictor is independent of other predictors. It is based on assumption of independence predictors.



It can be build easily with no iterative parameter estimation.



$$P(c \mid X) = P(x_1 \mid c) \times P(x_2 \mid c) \times \cdots \times P(x_n \mid c) \times P(c)$$

where $P(c|x)$ is the posterior probability.

P(x|c) is likelihood.

P(c) is prior probability of class.

P(x) is prior probability of predictors.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

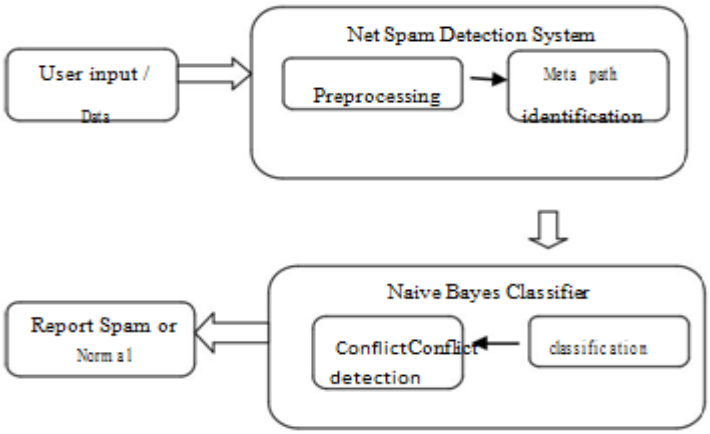
Vol. 8, Issue 3, March 2019

Algorithm

```
TRAINMULTINOMIALNB(C, D)
 1  V ← EXTRACTVOCABULARY(D)
 2  N ← COUNTDOCS(D)
 3  for each c ∈ C
 4  do N_c ← COUNTDOCSINCLASS(D, c)
 5     prior[c] ← N_c/N
 6     text_c ← CONCATENATETEXTOFALLD(
 7     for each t ∈ V
 8     do T_ct ← COUNTTOKENSOFTERM(tex
 9     for each t ∈ V
10     do condprob[t][c] ← (T_ct+1) / Σ_t'(T_ct'+1)
11  return V, prior, condprob

APPLYMULTINOMIALNB(C, V, prior, condprob,
1  W ← EXTRACTTOKENSFROMDOC(V, d)
2  for each c ∈ C
3  do score[c] ← log prior[c]
4     for each t ∈ W
5     do score[c] += log condprob[t][c]
6  return arg max_c∈C score[c]
```

V. ARCHITECTURAL DIAGRAM



VI. FUTURE WORK

The future system may be enhanced by providing various security breaches while creating an account for any social media. The security breaches may be finger print. By that individual person can create only one account to avoid fake accounts in any social media.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

VII. CONCLUSION

In existing system detection has been done on user based features or content based features but, all the approaches are valid only for small data set and not tested between spammer and non spammer. The experimental result shows that the proposed system yield good accuracy. The use of Bayesian network reduce noisy data and increase performance and also send an alert message to the users who receive the spam messages at the beginning of the conversation.

REFERENCES

1. N.K. Alex Cheng, Mark Evans, Inside the Political Twitter sphere, Sysomos. (2009). (accessed February5, 2017).
2. Chao Chen, Jun Zhang, Member, IEEE, Yi Xie, Yang Xiang,Senior Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Mohammad Mehedi Hassan, Abdulhameed AlElaiwi, and Majed Alrubaian, "A Performance Evolution of Machine Learning-Based Streaming Spam Tweets
3. Detection," IEEE Transactions on Computational Social Systems , 2016.
4. M. Chakraborty, S. Pal, R. Pramanik, and C.Ravindranth Chowdary,
5. "Recent developments in social spam detection and combating techniques: Asurvey," Inf. Process. Manag., 2016.
6. Chao Yang, Robert Harkreader, Jialong Zhang, Suengwon Shin, and Guofei
7. Gu.Analyzing Spammers' Social Networks For Fun and Profit – A Case Study ofCyber Criminal Ecosystem on Twitter.
8. T. Huddleston, Now Twitter Wants You to Create Your Own"Moments,"
9. Fortune.(2016).
10. R. Hassanzadeh. Anomaly Detection in Online Social Networks: Using Datamining Techniques and Fuzzy Logic. Queensland University of Technology, Nov. 2014.
11. Kayode Sakariyah Adewole, Nor Badrul Anuar, AmirrudinKamsin, Kasturi Dewi Varathan, Syed Abdul Razak,
12. "Maliciousaccounts:Dark of the social \networks,"Journal of Network andComputer Applications 79 , 41–67, 2017.
13. R. Shebuti and L. Akoglu. Collective opinion spam detection: bridgingreview networksand metadata. In ACM KDD, 2015.
14. H. Wang, "Don't follow me: Spam detection in twitter," in Proc.SECRYPT, Athens, 2010, pp. 1–10.
15. Y. Zhu, X. Wang, E. Zhong, N. Liu,H.Li,andQ.Yang,"Discoveringspammers in social networks," in Proc. AAAI-12, Toronto, Ontario, 2012,pp. 52–58.