Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 5, May -2016

An Improved Method for Spam Detection in Social Media

Ms. Hetal Shah [1], Mr. Krunal Patel[2]

[1]Department of Computer Science and Engineering, PIT Vadodara,
[2]Department of Computer Science and Engineering, PIT Vadodara,

Abstract – *Social network has become a very popular way for internet users to communicate and interact online. Users spend plenty of time on famous social networks (e.g., Facebook, Twitter, etc.), reading news, discussing events and posting messages. Unfortunately, this popularity also attracts a significant amount of spammers who continuously expose malicious behavior (e.g., post messages containing commercial URLs, following a larger amount of users, etc.), leading to great misunderstanding and inconvenience on users' social activities. Hence, we have studied a supervised machine learning and based on that, solution is proposed for an effective spammer detection. The traditional procedure for work is to collect a dataset and then construct a modeled based dataset and manually classify the users. It is quite time consuming. So, we have proposed a system which would comprise of Bagging and Boosting for classification along with Support Vector Machine.*

Keywords – *Social Media, Spam, Support Vector Machine, Bagging, Boosting, Feature Vectors.*

I. INTRODUCTION

Generally, data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.
Data mining consists of five major elements:

- Extract, transform, and load transaction data onto the data warehouse system.
- Store and manage the data in a multidimensional database system.
- Provide data access to business analysts and information technology professionals.
- Analyze the data by application software.
- Present the data in a useful format, such as a graph or table.

The impact of social spam is already significant. A social spam message is potentially seen by all the followers and recipients' friends. Even worse, it might cause misdirection and misunderstanding in public and trending topic discussions. For example, trending topics are always abused by spammers to publish comments with URLs, misdirecting all kinds of users to completely unrelated websites. Because most social networks provide shorten service on URLs inside message, it is difficult to identify the content without visiting the site. There has been a few proposals from industry and academia, discussing possible solutions for spam detection and filtering. However, they are either ineffective or based on too much considered conditions (e.g., a lot of content and behavior feature, etc.)[1].
Globally 75.9% of email messages are spam. Similarly, for the social networks the current state of spam is worsening and more rigorous efforts are required to stop them in an effective manner. Nowadays, spammers are trying a new approach to gain access through Facebook events. Generally, Facebook events are used by the spammers to invite users with bogus titles, e.g., "check out who viewed your profile." Although, these links direct to valid Facebook event pages, once a user views more information, the malicious link is displayed . Similarly, botnets, worms, and viruses have emerged on OSNs. The study of spam done point out different strategies used by bots to launch successful spam campaigns. Such spam campaigns consists of a single spammer having multiple accounts on OSNs, which increases the chance of a user being exposed to spam[2].

II. SPAM DETECTION IN SOCIAL MEDIA

The main objective for spam detection is its widespread prevalence in each and every field relating to social media. Where ever there is social network, there are some of the drawbacks such as intruders, attackers, hackers, etc. who try to steal our data and include spam. Spams are not only a hindrance but it also is a misleading thing which can create a lot of problems to people using social media.
Our objective is to detect such spam and to do so for a huge amount of data with higher level of accuracy and in a time-efficient manner.

III. SUPPORT VECTOR MACHINE FOR CLASSIFICATION

In machine learning, support vector machines are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked for belonging

to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on [16].
In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.
When data are not labeled, supervised learning is not possible, and an unsupervised learning approach is required, which attempts to find natural clustering of the data to groups, and then map new data to these formed groups. The clustering algorithm which provides an improvement to the support vector machines is called support vector clustering and is often used in industrial applications either when data is not labeled or when only some data is labeled as a preprocessing for a classification pass[16].

Advantages of using Support Vector Machines [16]

SVMs can be used to solve various real world problems:

- SVMs are helpful in text and hypertext categorization as their application can significantly reduce the need for labeled training instances in both the standard inductive and transductive settings.
- Classification of images can also be performed using SVMs. Experimental results show that SVMs achieve significantly higher search accuracy than traditional query refinement schemes after just three to four rounds of relevance feedback.
- SVMs are also useful in medical science to classify proteins with up to 90% of the compounds classified correctly.
- Hand-written characters can be recognized using SVM.

Disadvantages of Support Vector Machines

It takes almost an hour or more in the process of model training for even a small dataset. Hence, the biggest limitation is time.

IV. RELATED WORK

There are following papers referred as the literature survey. These all papers include the advantages and limitations.

A. Detecting Spammers on Social Networks[1]

In this paper, a supervised machine learning based solution is proposed for an effective spammer detection. The main procedure of the work is: first, collect a dataset from Sina Weibo including 30,116 users and more than 16 million messages. Then, construct a labeled dataset of users and manually classify users into spammers and non-spammers. Afterwards, extract a set of feature from message content and users' social behavior, and apply into SVM (Support Vector Machines) based spammer detection algorithm. The experiment shows that the proposed solution is capable to provide excellent performance with true positive rate of spammers and non-spammers reaching 99.1% and 99.9%respectively

B. A Generic Statistical Approach for Spam Detection in Online Social Networks [9]

The study is based on real datasets containing both normal and spam profiles crawled from Facebook and Tweeter networks. We have identified a set of 14 generic statistical features to identify spam profiles. The identified features are common to both Facebook and Twitter networks. For classification task, we have used three different classification algorithms Naive Bayes, Jrip, and J48, and evaluated them on both individual and combined datasets to establish the discriminative property of the identified features.[2].
described spam detection techniques, different steps for spam detection. In the fifth section described methodology of spam detection and then the different spam feature extraction [2].

C. Spam Detection and Filtration using Data Mining for Social Networking Sites [2]

The complete process is divided into six tasks explained as follows:
Task 1: First of all we have to extract and fetch the Facebook comments to our local machine.
Task 2: After storing comments we need to parse each comment.
Task 3: Next to parsing of data is the tokenizing of comments for proper structuring.
Task 4: After tokenization of the comments we need to check for its spam classification. If it contains URL check for suspicious URLs (URL Features: Number of (.), special URLs etc.) If it not contains URL check for suspicious word by comparing with spam keyword stored in database.
Task 5: Determine whether a comment on aspect is spam, no spam or neutral.
Task 6 Produce all messages expressed in document based on results of the above tasks
This paper Demonstrates the data mining approach on OSNs [2] (Online Social Networks) to detect the spam on data generated from feedbacks, comments to produce a categorized summary of messages. For the spam detection, the spam

word dataset, URL blocking, keyword blocking is applied on rendered message. Then, the data mining or text classification algorithm is used to detect the overall spam [3].

D. Techniques to Detect Spammers in Twitter-A Survey[4]

In this paper the techniques available for detection of spammers in Twitter have been presented along with their analysis and comparison. This paper is structured as follows: Section 2 describes methodology used to carry out this review; followed security issues in OSNs which have been briefed in Section 3; Section 4 presents definition of spammers and their motives; Introduction to Twitter and its threats has been covered in Section 5; Section 6 is about the motivation behind this survey paper; Section 7 covers the attributes that can be used for detection purpose; Section 8 reviews the work done by various researchers with a comparative analysis [4].

V. PROPOSED WORK

From the papers reviewed it can be concluded that most of the work has been done using classification approaches like SVM, Decision Tree, Naive Bayesian, and Random Forest. Detection has been done on the basis of user based features or content based features or a combination of both. We have also introduced new features for detection. All the approaches have been validated on very small dataset and have not been even tested with different combinations of spammers and non-spammers. Combination of features for detection of spammers has shown better performance in terms of accuracy, precision, recall etc. as compared to using only user based or content based features.

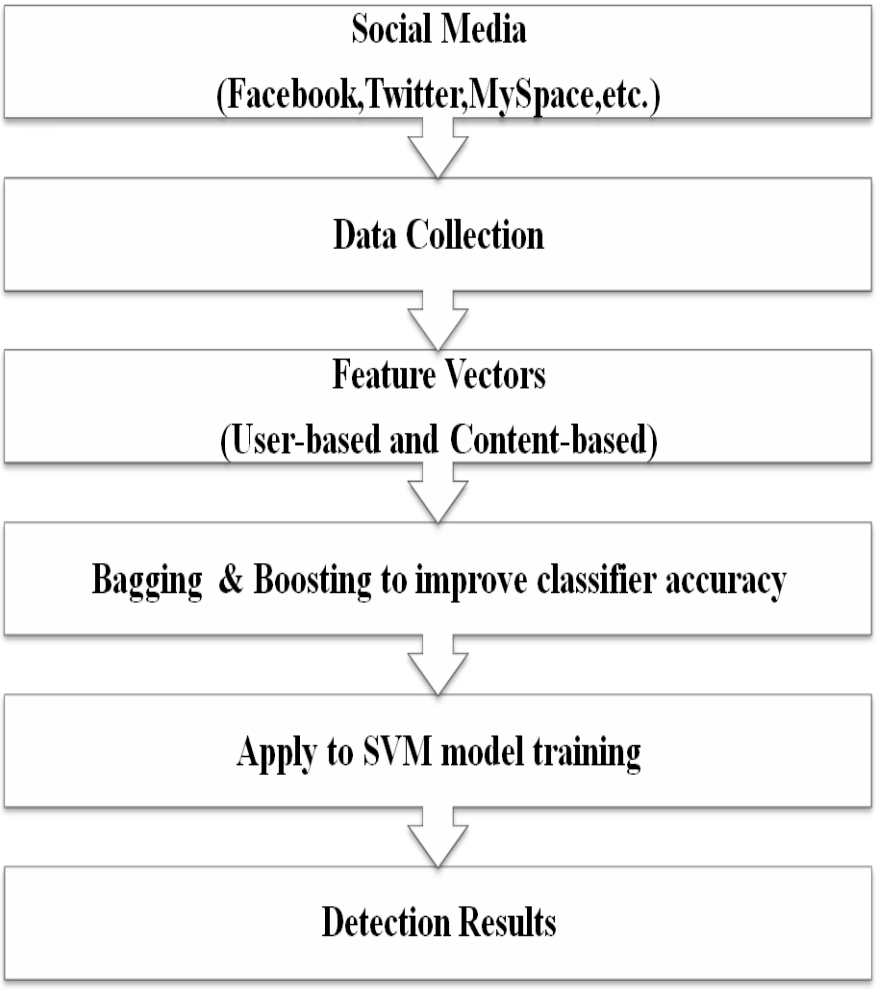

Figure 1: Block Diagram of Proposed Work

VI. CONCLUSION

The Support Vector Machine method is one of the best approaches for classification in spam detection. We have analyzed the drawbacks and tried to propose a new approach that overcomes the drawbacks of conventional methods. The bagging and boosting methods help us train the model quite faster and hence improving efficiency along with accuracy.

A new proposed approach is designed for spam detection that gives more accurate result along with less time and manual efforts.

REFERENCES

[1] Xianghan Zhen, Zhipeng Zeng, Zheyi Chen, Yuanlong Yu, Chunming Rong, "Detecting Spammers On Social Networks", Elsevier Neurocomputing 159 27–34 2015.

[2] Ritesh Kumar, Mayur Girnar, Archana Darwatkar, Shital Ghadage, Prof. G.S Navale, "Spam Detection and Filtration using Data Mining for Social Networking Sites", International Journal Of Scientific Progress And Research (IJSPR) ,Volume-10, Number - 01, 2015.

[3] Michael Fire, Member, IEEE, Roy Goldschmidt, and Yuval Elovici, "Online Social Networks: Threats and Solutions", IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014.

[4] Monika Verma, Divya, Sanjeev Sofat, " Techniques to Detect Spammers in Twitter- A Survey", International Journal of Computer Applications,Volume 85 – No 10, January 2014.

[5] Michael Crawford, Taghi M. Khoshgoftaar, Joseph D. Prusa, Aaron N. Richter and Hamzah Al Najada, "Survey Of Review Spam Detection Using Machine Learning Techniques", Crawford et al. Journal of Big Data , DOI 10.1186/s40537-015-0029-9, 2015.

[6] Yang Song, Aleksander Kołcz and C. Lee Giles, "Better Naive Bayes Classification For High-Precision Spam Detection", SOFTWARE—PRACTICE AND EXPERIENCE Softw. Pract. Exper. 2009; 39:1003–1024 Published online 22 April 2009.

[7] Sahil Puri , Dishant Gosain , Mehak Ahuja, Ishita Kathuria, Nishtha Jatana, "Comparison And Analysis Of Spam Detection Algorithms", International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 - 4847 Volume 2, Issue 4, April 2013.

[8] Vandana Jaswal, Astt Professor. Nidhi Sood, "Spam Detection System Using Hidden Markov Model", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, ISSN: 2277 128X, July 2013.

[9] Faraz Ahmed and Muhammad Abulaish, "A Generic Statistical Approach for Spam Detection in Online Social Networks", Computer Communications, 36(10-11), Elsevier, pp. 1120-1129, 2013.

[10] Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia, Alok Choudhary, "Towards Online Spam Filtering in Social Networks", downloaded from http://users.eecs.northwestern.edu/~kml649/publication/GaoChe12.

[11] Xin Chen, Mihaela Vorvoreanu, and Krishna Madhavan, "Mining Social Media Data for Understanding Students' Learning Experiences", IEEE Transactions On Learning Technologies, Vol. 7, No. 3, July-September 2014.

[12] Bing Liu, "Detecting Fake Opinions in Social Media", Department of Computer Science, University Of Illinois at Chicago.

[13] X. Jin, C. Lin, J. Luo, J. Han, "A data mining-based spam detection system for social media networks", Proceedings of the VLDB Endowment, 4(12):1458-1461; 08/2011.

[14] Xuchun Li, Lei Wang, Eric Sung "AdaBoost with SVM-based component classifiers", ELSEVIER, Engineering Applications of Artificial Intelligence 21 (2008) 785–795

[15] S.M. Valiollahzadeh; A. Sayadiyan; and F. Karbassian,"Adaptive Boosting of Support Vector Machine Component Classifiers Applied in Face Detection"

[16] https://en.wikipedia.org/wiki/Support_vector_machine

