IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 05, Issue 09 (September. 2015), ||V1|| PP 32-34

Predicting spam videos using predictive analysis.

P. Sai Kiran, Dathala Irwin Emmanuel
(Computer Science and Engineering, Vidya Jyothi Institute of Technology(JNTU-H), TG, India)
(Computer Science and Engineering, Vidya Jyothi Institute of Technology(JNTU-H), TG, India)

Abstract: Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Facebook, MySpace, or Twitter), storing and sharing personal information. This information, also attracts the interest of cybercriminals.
There has been a lot of development regarding spam detection in the recent times. This paper tries to address, if there is a way to leave off a video in a social video platform without checking if it is spam or not. That is, predicting if it is spam or not.

Keywords*: YouTube, Spammers, video spam, social network, Supervised Machine Learning, Machine Learning, SVM, video predictions, predictive analysis.*

I. INTRODUCTION

Over the last few years, social networking sites have become one of the main ways for users to keep track and communicate with their friends online. Sites such as Facebook, MySpace, and Twitter are consistently among the top 20 most-visited sites of the Internet. Moreover, statistics show that, on average, users spend more time on popular social networking sites than on any other site [1]. Most social networks provide mobile platforms that allow users to access their services from mobile phones, making the access to these sites ubiquitous. The tremendous increase in popularity of social networking sites allows them to collect a huge amount of personal information about the users, their friends, and their habits. Unfortunately, this amount of information, as well as the ease with which one can reach many users, also attracted the interest of malicious parties. In particular, spammers are always looking for ways to reach new victims with their unsolicited messages. This is shown by a market survey about the user perception of spam over social networks, which shows that, in 2008, 83% of the users of social networks have received at least one unwanted friend request or message [2].

By allowing users to publicize and share their independently generated content, social video sharing systems may become susceptible to different types of malicious and opportunistic user actions, such as self-promotion, video aliasing and video spamming [3]. A video response spam is defined as a video posted as a response to an opening video, but whose content is completely unrelated to the opening video. Video spammers are motivated to spam in order to promote specific content, advertise to generate sales, disseminate pornography (often as an advertisement) or compromise the system reputation.

Ultimately, users cannot easily identify a video spam before watching at least a segment of it, thus consuming system resources, in particular bandwidth, and compromising user patience and satisfaction with the system. Thus, identifying video spam is a challenging problem in social video sharing systems.
The paper specifically addresses the issue, 'Do we really need to check every video and analyze to predict whether it's spam or not?'
What I am trying to accomplish is taking some attributes of the videos, attach some threshold values to the attributes which might lead to address the above question.
The rest of the paper is organized as follows, the next section would give an overview of the background followed by user test collection which discusses the method in which the test data was collected. Lastly, we have predictive analysis section which discusses the algorithm and the results.

II. BACKGROUND

Mechanisms to detect and identify spam and spammers have been largely studied in the context of web [4, 5] and email spamming [6]. In particular, Castillo et al [4] proposed a framework to detect web spamming which uses social network metrics. A framework to detect spamming in tagging systems, which is a type of attack that aims at raising the visibility of specific objects, was proposed in [7]. Although applicable to social media sharing systems that allow object tagging by users, such as YouTube, the proposed technique exploits a specific object attribute, i.e., its tags. A survey of approaches to combat spamming in Social web sites is presented in [8]. Many existing approaches are based on extracting evidence from the content of a text, treating the text corpus as a set of objects with associated attributes and using these attributes to detect spam.

These techniques, based on content classification, can be directly applied to textual information, and thus can be used to detect spam in email, text commentaries in blogs, forums, and online social networking sites. Complementary to my effort, the characterization of the traffic to online video sharing systems, in particular YouTube, has also been the focus of some studies. An in-depth analysis of popularity distribution, popularity evolution and content characteristics of YouTube and of a popular Korean video sharing service is presented in [9]. The authors also analyze mechanisms to improve video distribution, such as caching and peer-to-peer distribution schemes. Gill et al [10]present a characterization of the YouTube traffic collected from the University of Calgary campus network and compare its properties with those previously reported for web and media streaming workloads. Both studies focus on traffic and video characterization.

III. USER TEST COLLECTION

This paper is a continuation of my previous work in the same segment and many results are compared directly. The process of the user collection is same. The results are presented in [11].
Simultaneously attributes such as the number of likes, comments are collected additionally.

IV. PREDICTIVE ANALYSIS

Generically the videos whose view count is more than a threshold of 10,000 are found to be 85% non - spam when compared with the results from [11].

ALGORITHM:

input: A list of information about users.
1.1 Initialized threshold values for no_of_likes and viewcount;
1.2 foreach User U in info - list do
1.3 if likes greater than no_of_likes and view greater than viewcount then
1.4 do natural language processing on every comment;
1.5 if result is positive
1.6 label it as not spam;
1.7 end
1.8 if result is negative
1.9 label it as spam;
1.10 end
1.11 end
1.12 end

To increase the precision, attributes such as likes and comments are considered. A video which has more than 70% likes increases the precision to 90%. Additionally performing analysis using a natural language processing library such as Natural Language Toolkit [12] differentiating the positive and negative comments further increased the precision to 93.6%.

V. CONCLUSION

Deploying an automatic engine such as this will help the spam classifier engine to carefully omit some videos which are predicted to be not spam.
This will not only increase the efficiency but also ensures minimal use of resources.

Issues with this method:

For smaller data sets it has been observed that doing analysis on comments sometimes led to decrease in accuracy.
One of the methods to address this problem is to have a large data set for training SVMs.
My work in this will continue and in future I would work on the above mentioned issue.

REFERENCES

[1] Alexa top 500 global sites. http://www.alexa.com/topsites.
[2] Harris Interactive Public Relations Research. A study of social networks scams. 2008
[3] M. Cha, H. Kwak, P. Rodriguez, Y. Ahn, and S. Moon. I tube, you tube, everybody tubes: Analyzing the world's largest user generated content video system. In Proc. of IMC, 2007.
[4] C. Castillo, D. Donato, A. Gionis, V. Murdock, and F. Silvestri. Know your neighbors: Ib spam detection using the Ib topology. In Int'l ACM SIGIR, pages 423–430, 2007.
[5] Z. Gy¨ongyi, H. Garcia-Molina, and J. Pedersen. Combating Ib spam with trustrank. In Int'l. Conf. on Very Large Data Bases, pages 576–587, 2004.

[6] L. Gomes, F. Castro, V. Almeida, J. Almeida, R. Almeida, and L. Bettencourt. Improving spam detection based on structural similarity. In Proc. of SRUTI, 2005.
[7] G. Koutrika, F. Effendi, Z. Gy¨ongyi, P. Heymann, and H. Garcia-Molina. Combating spam in tagging systems. In Proc. of AIRIb, 2007.
[8] P. Heymann, G. Koutrika, and H. Garcia-Molina. Fighting spam on social Ib sites: A survey of approaches and future challenges. IEEE Internet Computing, 11(6):36–45, 2007.
[9] M. Cha, H. Kwak, P. Rodriguez, Y. Ahn, and S. Moon. I tube, you tube, everybody tubes: Analyzing the world's largest user generated content video system. In Proc. of IMC, 2007.
[10] P. Gill, M. Arlitt, Z. Li, and A. Mahanti. YouTube traffic characterization: A view from the edge. In Proc. of IMC, 2007.
[11] P. Sai Kiran. Detecting spammers in YouTube: A study to find spam content in a video platform. ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 05, Issue 07 (July. 2015), ||V4|| PP 26-30.
[12] Natural Language Toolkit. http://www.nltk.org