www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21209-21211
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.04

Naïve Tweet Analyser

Abhinav Garg[1], Kratika Gupta[2], Abhijeet Singh[3]

[1,2,3]Department Of Computer Science, Galgotias College Of Engineering And Technology, Greater Noida, India

Abstract

Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. Conventional Twitter spam detection schemes utilize account features such as the ratio of tweets containing URLs and the account creation date, or relation features in the Twitter graph. The techniques misses' one major factor in the assessment and that is the content of the tweets. So basically we have developed software which on the basis of content of the tweet classifies using naïve bayes classifier whether the tweet is positive or negative. Also we have gone a level up with this software and that is, not only profile specific assessment of tweets can be done but also a person can search for words and look into the tweets that contain the word twitter wide to get individual assessment of the tweets as well as overall statistical data in form of a pie chart. Content specific assessment is important because one can have a verified twitter account with all the technical parameters satisfying and can still spread malicious content or the account could be hacked in to spread malicious content. For the solution, we have come up with the software.

Keywords : Twitter, Malicious, Naïve Bayes classifier, Spam, Pie chart

1. Introduction

Social networking sites have become one of the main ways for users to keep track and communicate with their friends online. Sites such as Face book, MySpace, and Twitter[2] are consistently among the top 20 most-viewed web sites of the Internet. Social networking websites are significant pieces of everyday's life from the last few years. People take help of social networking sites where they are easily associated with their family members and billions of people from the whole globe. But those social situations are not just only used to partake in their sentiments, but some people use it for doing their unauthorized activities by which public gets disturbed or hack their system and access their individual data. Twitter is a micro blogging service nearly 11 years old, command more than 314 million users as of a recent survey and is growing fast. Twitter users tweet about any topic within the 140-character limit also know as tweets and follow others to receive their tweets. It has over 100 million dynamic users who place about 200 million tweets everyday.

As twitter is such widely used platform, there comes an important factor of security. There are various attacks possible such as phishing attacks, spam. loss of identity, hacking, spreading of malicious content etc. There are various software or systems, such as warningbird[4], malicious tweet url blocker etc, developed to avoid these attacks. The techniques used by these software's focuses on some technical factors such as correlation of URL redirect chain extracted from number of tweets, initial URLs, similar tweet texts, a number of accounts, similar follower friend ratio, bit of landing URLs etc . These softwares are very good in their particular perspective but the one major thing they miss is that none focuses on the content of the tweets. Let us imagine a scenario, there is a verified account of a famous personality on twitter, so when we look at the aspects such as friend follower ratio etc the outcomes come out to be correct and no malicious tweet could possibly be detected. But what if the account is possibly hacked and some malicious content is being spread by it. So, we realize that content based filtering is also important. For this purpose we have developed this software.

The major concepts used in this project are web crawling and naïve bayes classifier. A web crawler precisely is a program that downloads and stores webpages ,often for a web search engine. A crawler starts off by placing an initial set of urls, called seed urls into the queue where all urls to be retrieved are kept and prioritized . From this queue crawler gets an urls , downloads the page and extracts any url's in the downloaded page and pass the new urls in queue. Crawling[3] is basically looking into the web page, reading it and then further gathering the urls found in that page and repeating the process. This concept is used in this software. Naive Bayes classifiers are a family of simple probabilistic

DOI: 10.18535/ijecs/v6i5.04

classifiers based on applying Bayes' theorem with strong (naive) independence assumptions between the features. Bayesian classification provides practical learning algorithms and prior knowledge and observed data can be combined. Bayesian Classification provides a useful perspective for understanding and evaluating many learning algorithms. It calculates explicit probabilities for hypothesis and it is robust to noise in input data

. For a document d and a class c,

$$P(c, d) = P(c|d)\,P(d) = P(d|c)\,P(c)$$

$$P(c|d) = P(d|c)\,P(c)\,/\,P(d)$$

Using these two major concepts the software works. The flow of which being, when we run the software a window opens with a search option, typing the word or the account holder's twitter handle and pressing of search fetches us all the tweets all over the twitter. Further the content of the tweet is assessed. If the tweet contains any URL then the crawling concept comes into play. Classification of the url and text as positive or negative comes up as well as a pie chart representing the statistics is displayed.

In this software not only an user's account tweets can be checked but also the tweets present all over twitter having the word searched can be accounted for statistics.

2 .LITERATURE SURVEY

Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware[1] distribution. Many steps have been taken and many softwares' have been developed to fight against it.

T.Lakshmi, S.Parthiban [5] have proposed a system "warning bird" for detection of malicious tweets on twitter. Unlike the conventional systems, WARNINGBIRD is robust when protecting against conditional redirection, because it does not rely on the features of malicious landing pages that may not be reachable. Instead, it focuses on the correlations of multiple redirect chains that share the same redirection servers. Because attackers have limited resources and usually reuse them, their URL redirect chains frequently share the same URLs. We develop methods to discover correlated URL redirect chains using the frequently shared URLs and to determine their suspiciousness. We collect numerous tweets from the Twitter public timeline and build a statistical classifier using them. They introduced new features on the basis of these correlations implemented a near real-time classification system using these features, and evaluated the system's accuracy and performance. The evaluation results show that the system is highly accurate and can be deployed system to classify large samples of tweets from the Twitter public timeline.

Nupur S. Gawale, Nitin N. Patil[6] have also propsed a system. There system uses 5 factors for deciding whether an URL is malicious or not. 5 features like initial URLs, similar tweet texts, a number of accounts, similar follower friend ratio, and bit of landing URLs etc. In which first feature is initial URLs means the initial landing page or URL checked. Because the many times initial pages are same of that entry point URL. Then second feature is similar tweet text again in that same URL has the same text with a different URL, and also some URL with text both are same. Then side by side feature is account date means at which date tweets were downloaded from accounts. Afterward that the friend, follower ratio in this characteristic, the friend and follower of that every account should consider. And last feature is relative URLs, in which the URLs which are related to suspicious URLs. All this features applying in training module. And compare the non-suspicious URLs with the suspicious URLs. Ultimately, at the end it moves over the classification of suspicious and non-suspicious URLs. 94 % accuracy proves to be a better one from the security point of view.

As we have seen a lot of work has been done on security of twitter but the main focus was on technical aspects. Getting inspiration from this our software classifies tweets on the basis of the content.

3. METHODOLOGY

Over the last few years, there is tremendous use of online social networking sites. It's also providing opportunities for hackers to enter easily in network and do their unauthorized activities. This software is an attempt to analyse the tweets and to give statistical analysis.

The methodology used in this program is that firstly we create a web page which has a textbox and a search button. From here we offer 3 searching options:

1. Search a random word.
2. Tweets of a specific account
3. Tweets of a specific account with specific word.

The 1st option helps us to search a specific word in the tweets present all over twitter and then analyse those tweets.

The 2nd option allows us to analyse tweets of the specific account by entering the twitter handle name.

The 3rd option allows us to enter a twitter handle and a keyword which in turn returns the tweets of that account holder which contain the keyword searched.

DOI: 10.18535/ijecs/v6i5.04

After we have entered an pressed the search button the software searched for data into twitter and fetches data. After the data is fetched then the analysis part initiates. First of all the tweets are read and if they contain any url then these are separated ie, the text part is analysed separately and the URL part is analysed separately. For the classification of the tweets we have used the naïve bayes classifier. The data undergoes classification process. The text part is analysed by the naïve bayes classifier by the predefined datasets present. Now for the URL part, if present, we use the concept of a web crawler ie, from the given URL we fetch the data present and classify that data on the basis of the data sets present though naïve bayes classifier.

After this analysis is done we end up with the results of the text and URL. On the final page, the result is displayed as pie chart also in the second half of the page description of the tweets ,text part and url, and their analysis, positive or negative, is displayed.

The major concepts used in this project are web crawling and naïve bayes classifier. Content specific assessment is important because one can have a verified twitter account with all the technical parameters satisfying and can still spread malicious content or the account could be hacked in to spread malicious content. For the solution, we have come up with the software.

4. Future Scope

A lot of work has been done for filtering of malicious tweets or urls on twitter. While this is first of its kind where instead of some factors like friend follower ratio, friend list etc, content of the tweet is the factor of classification. A lot of opportunities in this field are there since this is a basic version. Improvement of the database such as inclusion of slang, hinglish terms etc. Also improvements can be made in the choice of a classifier. A classifier better than naïve bayes can be chosen and can be worked upon.

5.Conclusion

Various softwares such as warning bird have been developed to target malicious tweets and urls. The target of this software remains the same but the difference lies in the approach. On one hand where softwares like warning bird use technical features and aspects, our software is based on content. Content based filtering is an important phenomenon because while we are focusing on important aspects we have forgotten a very important factor that is the content. There is a possibility that these factors for an account come out to be correct still the content could be malicious, for this purpose this software has been developed. With the help of naïve bayes classifier we analyse the content of each tweet and classify them based on the database that we have created. Overall the results of the software are good but still improvements can be done for further better results.

6. References

[1] G. Stringhini, C. Kruegel, and G. Vigna, "**Detecting spammers on social networks**," *in Proc. ACSAC, 2010*.

[2] H. Kwak, C. Lee, H. Park, and S. Moon, "**What is Twitter, a social network or a news media?***" 19th international conference on World wide web, ACM, pp.591-600, April 2010.*

[3] Pavalam, S. M., SV Kashmir Raja, Felix K. Akorli, and M. Jawahar, "**A Survey of Web Crawler Algorithms**," *International Journal of Computer Science, vol. 8, iss. 6, no 1, Nov. 2011*.

[4] S. Lee and j. Kim*, "***Warningbird: Detecting Suspicious Urls In Twitter Stream***," in proc. ndss, 2012*

[5] T.Lakshmi, S.Parthiban, "**Warning Bird Mail Alert Based Malicious URLs Blocker System in Twitter**", *International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014*

[6] Nupur S. Gawale, Nitin N. Patil, "**Implementation of A System To Detect Malicious URLs for Twitter Users**", *2015 International Conference on Pervasive Computing (ICPC)*