Classifying Followers of the Most Influential Users on Twitter

Manoj Narayan Bisarahalli, Ramya Rajendra, Sahana Shreedhar Kulkarni

Abstract

Twitter is an application playing dual roles of microblogging and online social networking. Users publish text-based posts known as tweets. The open structure and popularity of Twitter have attracted bots, which appear to be a double-edged sword to Twitter. Bots have become a part of twitter, but determining how widespread they are can be tricky. Therefore the proposed system tries to predict the bot that spam on influential users' account.The system inputs names of two influential users and returns a graph indicating the bots among their common neighbors. Different ML algorithms are used for training the data: Logistic regression, Decision tree and Random forest.

Introduction

Twitter has become a popular microblogging service in recent years. About 200 million tweets are generated per day. Each user has a provision to share information with their friends or public in the form of text for up to 140 characters, which are popularly known as tweets. There is also a retweet mechanism that allows users to share information with their followers which can in turn help spread the information rapidly. This creates a massive celebrity-centric social network ,which plays a major role in breaking news, controversial opinions on issues and latest events. Such accounts must be given importance to understand the social network and how the users are influenced. Therefore ,on analyzing when and what the followers comment on tweets of these influential users and who they follow ,we can discover differential temporal patterns that can help us in classifying the followers as spammers or normal.

Related Work

Paper 1:

*Topic :*Detection of spam-posting accounts on Twitter
Author: Isa Inuwa-Dutse, Mark Liptrott, Ioannis Korkontzelos

Summary :

This paper talks about the approach for distinguishing spam and non-spam social media posts and gives some insight into the behavior of spam users on Twitter detection of spam by considering the pairwise engagement with each user.The idea sounds similar to ours, whereas we are trying to find the bots among 2 influential users.[1]

Paper 2:

*Topic:*Detecting Social Spam Campaigns on Twitter
*Author:*Zi Chu, Indra Widjaja, and Haining Wang
Summary:

This paper has a collective perspective, and focuses on detecting spam campaigns that manipulate multiple accounts to spread spam on Twitter.It also designs an automatic classification system based on machine learning, and apply multiple features for classifying spam campaigns.This approach is similar to our approach.We are using various ML algorithms like logistic regression,random forest and decision tree.Our approach has collect the user data and we have added about 16 features to them.[2]

Paper 3:

*Topic:*Information assurance:detection of web spam attacks in social media
*Author:*Pang-Ning Tan, Feilong Chen, and Anil K Jain
Summary:

This paper shows a co-classification framework to simultaneously detect Web spam and spammers in social media Web sites based on their content and link-based features.Our approach has a list of verified users and non verified users of twitter.We have added a few features and analysed the data[3]

Paper 4:

*Topic:*Identifying Twitter Spam by Utilizing Random Forests
Author: Humza S. Haider
Summary:

This paper user the random forest method to classify spammers and non-spammers.This is similar to our approach in a way as we have also used various ML algorithms like :logistic regression,random forest and decision tree.Our approach also finds the bots among 2 influential users.[4]

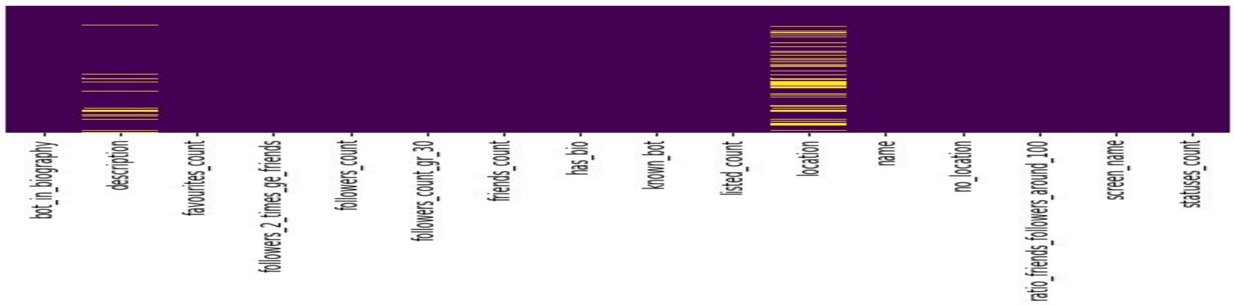
Paper 5:

*Topic:*Spam Detection on Twitter Using Traditional Classifiers
Author:M. McCord and M. Chuah
Summary:
This paper user the random forest method to classify spammers and non-spammers.This is similar to our approach as we have used various ML algorithms like :logistic regression,random forest and decision tree.Our approach has a list of verified users and non verified users of twitter.We have added a few features and analysed the data[5]

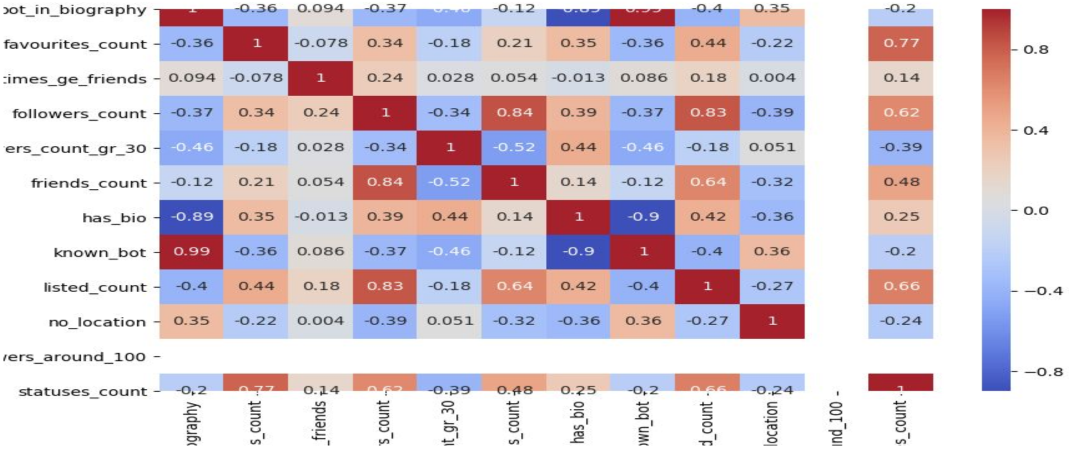
Approach

Our approach deals with classifying the followers of 2 influential users as spammers and normal users. There are two data sources: Data collected using Twitter API for a list of verified, non verified users and an existing dataset for bots and more real users.

In the process of building a model, the first step is data collection and processing. Here, the sklearn.preprocessing transformer methods are used to change raw feature data into a representation that is more suitable for the downstream estimators.



The above diagram shows a null value graph for the data collected. The various parameters that have been considered are: bot_in_biography, description, favourites_count, followers_2_times_ge_friends, followers_count, followers_count_gr_30, friends_count, has_bio, known_bot, listed_count, location, name, lo_location, ratio_friends_followers_around_100, screen_name and statuses_count. Among these, we can observe that description and location have a few null values.The heat map of the same is shown below.



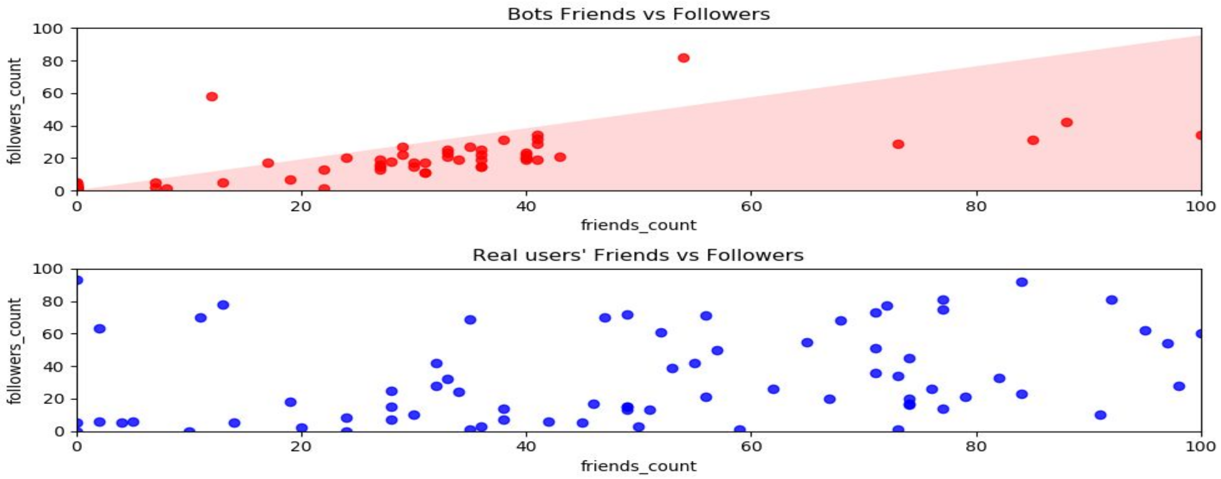
The libraries that we use are: sklearn, nltk, pandas, time, seaborn, pickle, json, click, numpy, twitterAPI and matplotlib.

As a part of the analysis of the data collected, to understand how certain features related to bots and real users are, we created some graphs shown in the experiment section. The total number of users collected are 2012 and 16 features per user.

In order to train the model,different ML algorithms are used such as Logistic regression, Decision trees and Random forest. For validation purposes we use K-fold cross validation.
Taking two influential users' screen names as input, the application crawls through the followers of two these two users and can find the common neighbors.The Decision tree model then predicts how many of these common neighbors are actually bots. Additionally, it signifies if these bot-like accounts target a group of influential users.

Experiment

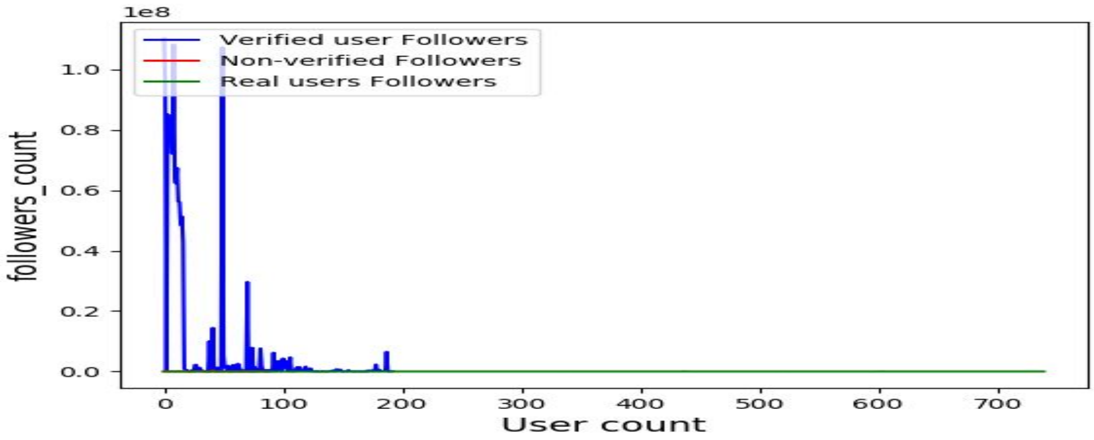
Experiments include training different ML based algorithms like :Logistic regression, Decision tree and Random forest. Categorical features are transformed and NaN or NULL values are replaced with a substitute string 'missing'. Mean accuracy is calculated for each of the classifiers with the use of K-folds for cross-validation.



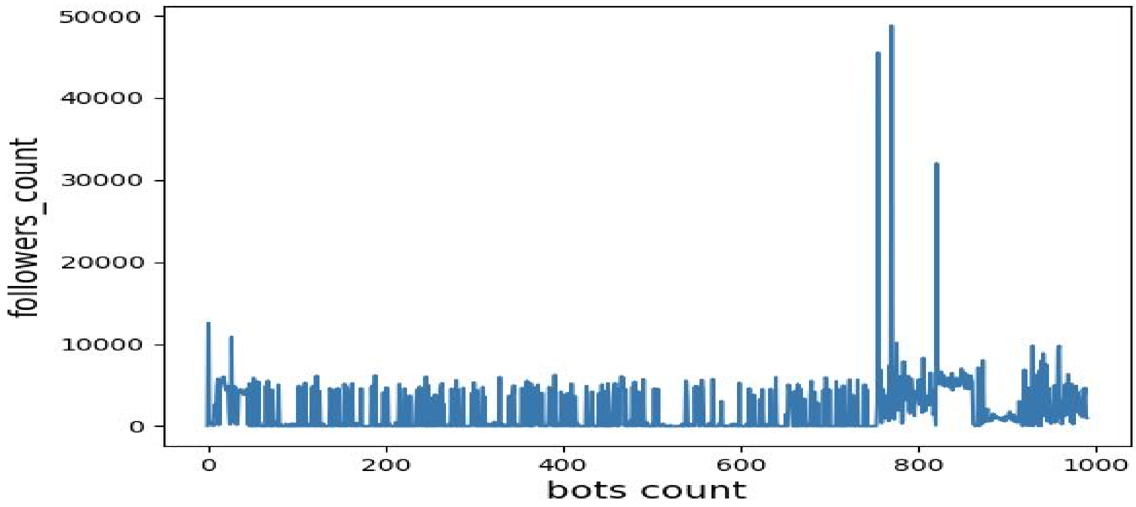
Consider the above two graphs.

In the first graph, Bot's friends v/s followers is analysed. Here the graph is plotted using the bots friends count against the followers count. We can observe how it's concentrated to one side.

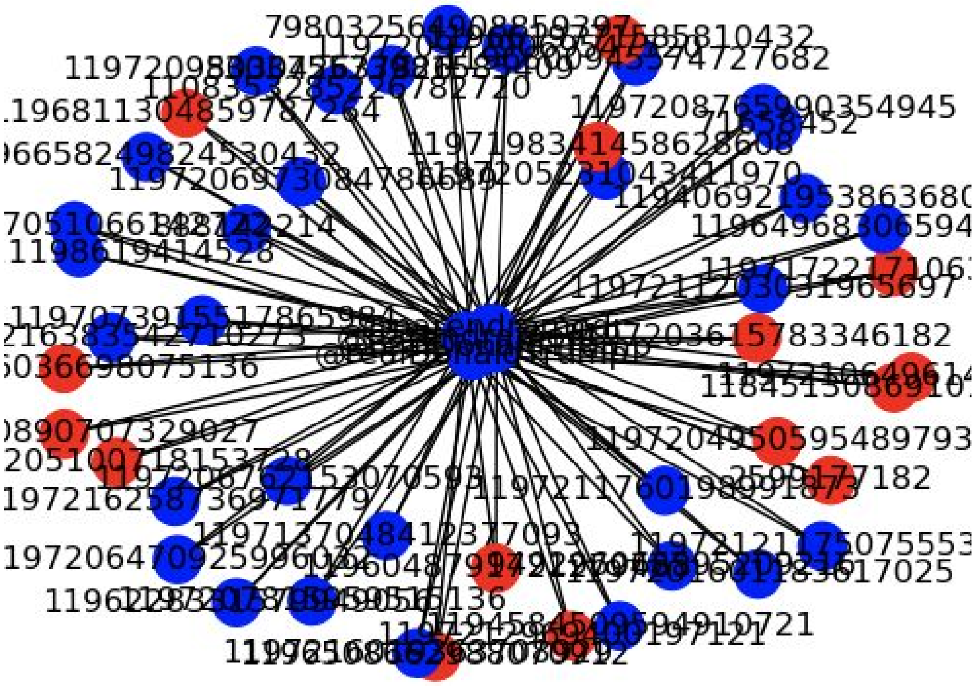
In the second graph, Real users' friends v/s followers is analysed. Here the graph is plotted using the real users' friends count against the followers count. We can observe how the users are distributed across the graph indicating the diverse number of friends and followers count for real users.



The above graph is plotted against the user count and followers count.From this we can infer that for real users the user count v/s follower count is almost constant, as indicated by the green line.Whereas, the verified user followers as indicated by the blue line tend to have high number of followers count.



The above line graph shows the variation of bots count v/s the followers count. As you can see, the followers count (y axis) magnitude is in 10,000s in contrast to verified users(10^8)



The above figure is the final result that is displayed the web app.The two user input that is @realDonaldTrump and @narendramodi is shown in the center. The common neighbors of these two users is shown along with the ID’s in blue. The bots identified by our model among them are indicated using red.

Conclusion

Analysis of a social network like Twitter to find common neighbors for influential users and build several classifiers to detect bots in this network are some of the main takeaways from the project.
Some future enhancements to the project can be as follows:

- More feature extraction and engineering. These features can be based on nature, tweet habits, followers count in short time stamp of the bot etc. Identify accounts with certain suspicious behavior as indication to investigate more.Behavior such as tweeting every few minutes in a full day, endorsing polarizing political propaganda (including fake news), obtaining a large follower account in a relatively small time span, and constant retweeting/promoting other bot accounts are all traits of bot accounts. These are the accounts that we aim to classify and bring to the attention.
- Another improvement can be to build models that identify different kinds of bots found on social media today.

References

[1] Detection of spam-posting accounts on Twitter, Isa Inuwa-Dutse, Mark Liptrott, Ioannis Korkontzelou
[2] Detecting Social Spam Campaigns on Twitter,Zi Chu, Indra Widjaja, and Haining Wang
[3] Information assurance:detection of web spam attacks in social media,Pang-Ning Tan, Feilong Chen, and Anil K Jain
[4] Identifying Twitter Spam by Utilizing Random Forests,Humza S. Haider
[5] Spam Detection on Twitter Using Traditional Classifiers,M. McCord and M. Chuah