

By:

Manoj Narayan Bisarahalli

Ramya Rajendra

Sahana Shreedhar Kulkarni



Abstract

 Trained a model that can classify a user as bot or not.

• For all the **common neighbors** of the given influential users, we find how many among them are bots.



Introduction

- Celebrity-centric social networks like Twitter play a major role
- Retweet mechanism can help spread information rapidly.
- Often popular accounts are considered in order to understand social network and how the users are influenced.
- Our system helps in profiling the followers of these influential users based on their behaviors and who they follow.



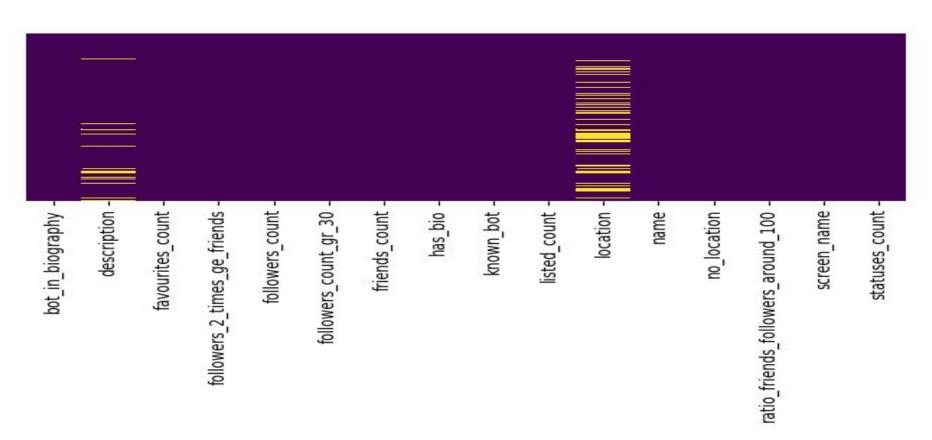
Approach |

Building the model

Data Collection and Preprocessing

The sklearn.preprocessing transformer methods are used to change raw feature data into a representation that is more suitable for the downstream estimators.

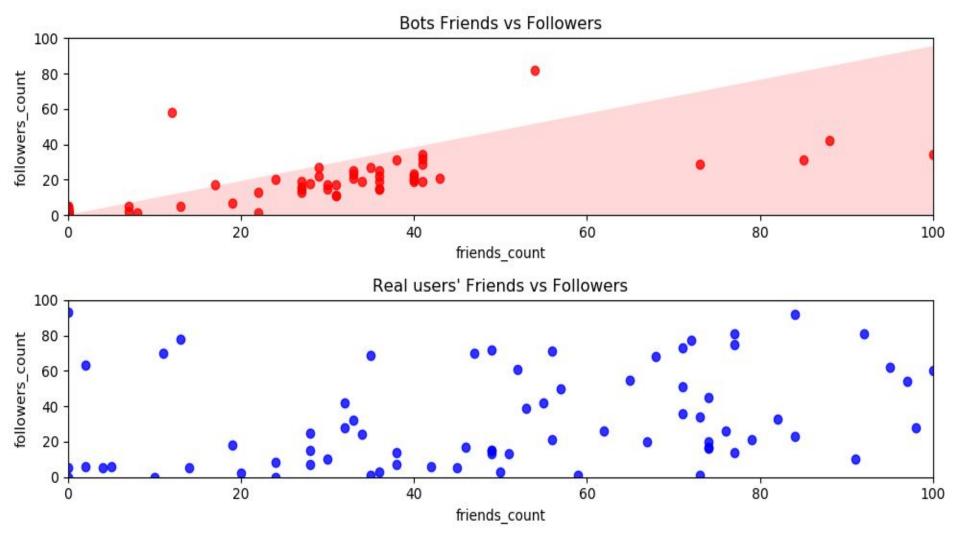
Null Values Graph

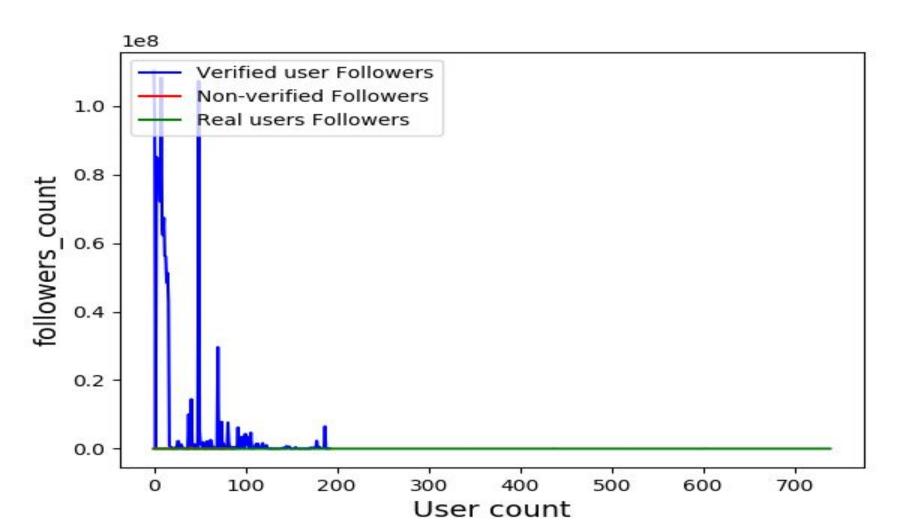




Analysis of Data Collected

- In order to understand how certain features related to bots and real users are, we created some graphs.
- Total number of users' collected : 2012
- Total features per user: 16







Model Training

- Different ML algorithms are been used for training the data:
 - Logistic regression
 - Decision tree
 - Random forest
- Used Kfold cross validation.
- Moving forward, we chose Decision tree for our web demo.



Application

 Crawled through the followers of two influential users and found common neighbors among them.

 Used our model to predict how many of these common neighbors are actually bots.

- Goal Find and classify bot-like followers of influential users.
 - Also signifies if these accounts target a group of influential users





Experiment

- For the datasets we have used live data as well as some existing dataset.
- New data(input) is been applied on the model: Logistic regression, Decision tree and Random forest as a part of experiment and the accuracy value is been obtained.
- The confidence value is been obtained and evaluated.



Conclusion

- The system is able to predict whether the given input (user) is a bot or not.
- The system is able to give a score as to how accurately the user can be called as a bot.
- The system is able to give a graphical representation of the influential users with the common neighbors.
- The system gives a line graph representation of the users v/s its followers.





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



Related Work

Paper 1:

Topic: Detection of spam-posting accounts on Twitter **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 analyze when and what the followers comment on tweet.

Paper 2:

Topic:Detecting Social Spam Campaigns on Twitter **Summary:**

This paper has a the 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. Our approach uses tf-idf (term frequency inverse document frequency) to systematically study commenting and retweeting behaviors of the followers and to discover different temporal commenting patterns and word diversity in the comments.



Related Work

Paper 3:

Topic:Information assurance:detection of web spam attacks in social media

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. We use two algorithms for classification: one is based on commenting behavior and patter and another with small number of comments based on know spammers and known normal fans.

Paper 4:

Topic:Identifying Twitter Spam by Utilizing Random Forests

Summary: This paper user the random forest method to classify spammers and non-spammers. We use two algorithms for classification: one is based on commenting behavior and patter and another with small number of comments based on know spammers and known normal fans. Our approach uses tf-idf (term frequency inverse document frequency) to systematically study commenting and retweeting behaviors of the followers and to discover different temporal commenting patterns and word diversity in the comments.



Related Work

• Paper 5:

Topic:Spam Detection on Twitter Using Traditional Classifiers

Summary:

This paper user the random forest method to classify spammers and non-spammers. We use two algorithms for classification: one is based on commenting behavior and patter and another with small number of comments based on know spammers and known normal fans. Our approach uses tf-idf (term frequency inverse document frequency) to systematically study commenting and retweeting behaviors of the followers and to discover different temporal commenting patterns and word diversity in the comments.