Bot detection in twitter landscape using unsupervised learning

Ahmed Anwar
ahmedanwar5295@gmail.com
Lahore University of Management Sciences

Ussama Yaqub
ussama.yaqub@lums.edu.pk
Lahore University of Management Sciences

ABSTRACT

The aim of this paper is to identify and understand bot activity in twitter discussion. The prevalence of Twitter bots have gained significant limelight recently due to their misuse in influencing public sentiment for political gains. For our analysis, we use Twitter data of 2019 Canadian Elections. We perform principal component analysis and K-means clustering on the data set. Using the results we isolate bots from human accounts.

CCS CONCEPTS

• **Information systems** → **Clustering**; *Social networks.*

KEYWORDS

Twitter, Social Media, Unsupervised learning, Clustering

ACM Reference Format:
Ahmed Anwar and Ussama Yaqub. 2020. Bot detection in twitter landscape using unsupervised learning. In *The 21st Annual International Conference on Digital Government Research (dg.o '20), June 15–19, 2020, Seoul, Republic of Korea.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3396956.3401801

1 INTRODUCTION

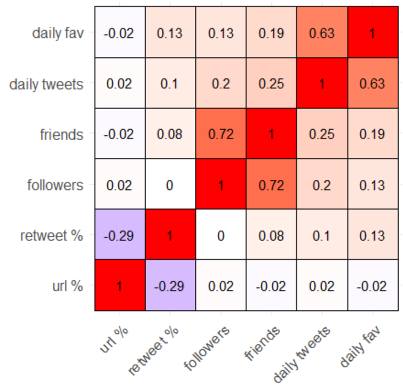
Twitter has become one of the most popular social media platform, with more than 321 million monthly users and 126 million daily users on average. This huge amount of user base, paved the way for the rise of social media bots which are aimed at influencing users for political purposes such as Russian Troll Farms during US Presidential Elections [1, 4]. Twitter data is unlabeled and hence it becomes difficult to classify twitter accounts as bots. This paper presents an unsupervised learning approach for detecting bots using twitter data from 2019 Canadian Elections.

2 DATA AND PREPOSSESSING

Twitter search API was used to accumulate 546,728 tweets pertaining to 2019 Canadian Elections from 103,791 unique users using the relevant search keywords. Attributes such as retweet, follower, status, daily tweets were extracted. Tweet text was dropped since our analysis was not based on text sentiment.

3 PRINCIPAL COMPONENT ANALYSIS

In total 13 attributes were selected from the twitter metadata. However, every feature was not equally representative of the total variance in the data set. Hence, we use correlation matrix and principal component analysis to check the relationship and importance of different variables.



	url %	retweet %	followers	friends	daily tweets	daily fav
daily fav	-0.02	0.13	0.13	0.19	0.63	1
daily tweets	0.02	0.1	0.2	0.25	1	0.63
friends	-0.02	0.08	0.72	1	0.25	0.19
followers	0.02	0	1	0.72	0.2	0.13
retweet %	-0.29	1	0	0.08	0.1	0.13
url %	1	-0.29	0.02	-0.02	0.02	-0.02

Figure 1: Correlation Matrix of Attributes

From figure 1, we find that attributes, such as daily favourites and daily tweets have a strong positive relationship. On the other hand, PCA plot of variables in figure 2 show features according to their explained variance relative to the overall variance. The closer an arrow is to the circumference, the greater variance is explained by it and vice versa. In addition, the direction of arrow depicts the direction of relationship.

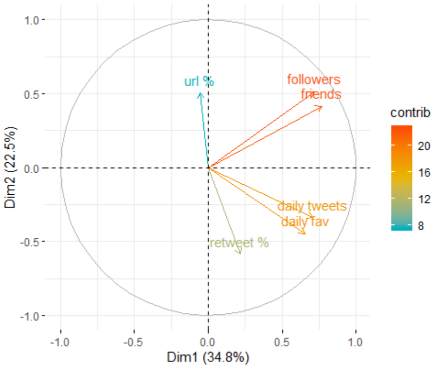


Figure 2: PCA of variables

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
dg.o '20, June 15–19, 2020, Seoul, Republic of Korea
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8791-0/20/06.
https://doi.org/10.1145/3396956.3401801

4 RESEARCH METHODOLOGY

In this section we discuss our research methodology. Since, our data set is unlabeled we used K-means clustering which is an unsupervised machine learning technique using sklearn package in python. This approach has also been used previously for hunting malicious bots in twitter campaigns [2, 3]. For clustering, we choose features of daily tweets, retweet percentage and daily favourite count. The number of clusters were set two, as our aim was to identify bots from humans.

5 EXPERIMENTAL RESULTS

This section showcases our findings. With the aid of unsupervised learning method, we created two clusters based on the three features. Clusters were labeled as Humans and bots, having 94% and 6% of total proportion respectively.

From table 1, we observe that though bots account for only a fraction of total tweets, their average number of daily tweets, retweet % and daily favourite are significantly higher than human accounts. For better visualization we created a 3d scatter (figure 3) in which bots have significantly higher values for retweet percentage and daily favourites. These findings are in line with the already identified characteristics of bot that bots accounts are small in number but their twitter discussion participation rate is very high [5–7].

Table 1: Mean Attributes for each Cluster

Cluster	Daily Tweets	Retweet %	Daily Fav
Human	12.35	0.694	12.81
Bots	136.06	0.865	164.47

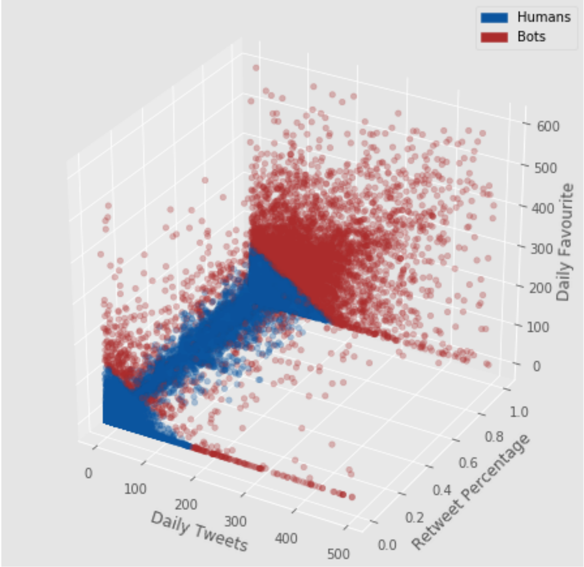


Figure 3: 3D Segmentation of bots

6 CONCLUSION AND FUTURE WORK

In this paper we used unsupervised machine learning to identify bots from Canadian Election tweets. Our approach presents a quick and inexpensive way of isolating bots from twitter discussion space.

In the future we would like to build upon this approach by incorporating twitter data sets of elections for different countries. This will take into account the demographic difference between countries and provide a universal method for bot identification.

REFERENCES

[1] David A Broniatowski, Amelia M Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C Quinn, and Mark Dredze. 2018. Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American journal of public health* 108, 10 (2018), 1378–1384.

[2] Zhouhan Chen and Devika Subramanian. 2018. An unsupervised approach to detect spam campaigns that use botnets on Twitter. *arXiv preprint arXiv:1804.05232* (2018).

[3] Zhouhan Chen, Rima S Tanash, Richard Stoll, and Devika Subramanian. 2017. Hunting malicious bots on twitter: An unsupervised approach. In *International Conference on Social Informatics*. Springer, 501–510.

[4] Stephen McCombie, Allon J. Uhlmann, and Sarah Morrison. 2020. The US 2016 presidential election & Russia's troll farms. *Intelligence and National Security* 35, 1 (2020), 95–114. https://doi.org/10.1080/02684527.2019.1673940 arXiv:https://doi.org/10.1080/02684527.2019.1673940

[5] Symantec Security ResponseSecurity Response Team, Symantec Security Response, AuthorSymantec Security ResponseSecurity Response TeamSymantec's Security Response, Symantec, and Symantec. [n.d.]. How to Spot a Twitter Bot.

[6] Ussama Yaqub, Soon Ae Chun, Vijayalakshmi Atluri, and Jaideep Vaidya. 2017. Analysis of political discourse on twitter in the context of the 2016 US presidential elections. *Government Information Quarterly* 34, 4 (2017), 613–626.

[7] Ussama Yaqub, Nitesh Sharma, Rachit Pabreja, Soon Ae Chun, Vijayalakshmi Atluri, and Jaideep Vaidya. 2020. Location-based Sentiment Analyses and Visualization of Twitter Election Data. *Digital Government: Research and Practice* 1, 2 (2020), 1–19.