

Fake Followers Detection on Twitter

¹Sunil Yadav, ²Mukul Maurya, ³Pratik Jaiswal

¹Head of Department, ^{2,3}U.G. Students
Shree L.R.Tiwari College of Engineering
Mumbai, Maharashtra, India

Abstract: Twitter is one of the most popular social networking platforms that people use to communicate and interrelate. Organization and companies use Twitter and other social media platforms, for the marketing and promotions of their products or services. To achieve this goal they seek to partner with Twitter influencers, as a part of their marketing strategy. Influencer marketing is considered more effective than traditional marketing. Influencers are more honest than a business due to the truth that they have developed close relationship with their followers.

Keywords: Twitter fake influencers, Networks, fake followers, classifier.

I. INTRODUCTION

Since the emergence of Internet in the current age, the number of users and its applications have enlarged to such an extent that Internet access has been declared as a fundamental right in various parts of the world. With this increase in practice, Social Networking platforms have become the main channel for all celebrities and organizations to reach their followers regarding their products, publicity and for marketing purposes. Bogus influencers are present across all major social platforms. Fake influencers have high engagement and size of the community. Influencer marketing has inflated in popularity and the ability to speak fake influencers has become severe to the continued success and trustworthiness of the market. Although some technique were proposed to detect fake Twitter accounts little effort has been dedicated to the detection of fake influencers.

II. RELATED WORK

[1] Pooja v Phad describes their system focuses on a set of tweets to build a user behavioural profile. A behavioural profile contains all tweets sent by a user and other things which are compulsory to post the tweet like application, time of tweet. Once they system gains the set of messages for each user, this data is used for building behavioural profile. Then system extracts feature values from each tweet and for each feature, feature model is trained. Based on a behavioural profile, they can regulate to what extent a new message follows the expected behaviour. They compute anomaly for each message and each feature value based on feature model. Each model gains feature value between [0, 1], where 0 shows perfectly normal feature and 1 shows extremely anomalous. After computing anomaly score for each feature, they must compute anomaly score for the whole message.

[2] According to Savvas Zinonos to conduct their experiential study they learned publicly accessible Twitter user egocentric networks. This is a very time-consuming process because for every Twitter account (ego) they sneaked they had to find all: • egos alters (followers and friends) • alter - alter ties. This means that for every single ego's alter they must find which of it alters (alters of alter) fit in to the set of ego's alters.

[3] Estée Van Der Walt There are many characteristics accessible in social media platforms that describe the identity of an SMP account. For example, the name, location, and profile image. Human accounts and bot accounts have similar characteristics and they share similar features. For example, human accounts have a name and so do accounts created by bots. Features can be engineered from social media platforms characteristics similar to what has been engineered in past research to detect fake accounts created by bots or computers (for example, whether the account is a identical of another).

Engineered features that have been created to detect fake identities generated by bots can be applied to the existing body of human accounts. The predictive results from the skilled machine learning models only produced a best F1 score of 49.75%. Given that predicting the correct answer by chance alone would be represented as 50%, this is not ideal. Even though only three machine learning models were used in the trials, these machine learning models have been positively used in the past towards spam and bot detection.

III. FINDING FAKE ACCOUNTS

In order to find a fake account created by human, first we should provide our machine learning model with fake account created by us so that the algorithm may know what a fake account is.

First we will clear all our previous data which was collected to find fake accounts created by bots or cyborg accounts as we want to find those accounts which are created by humans.

We came to know from our research that most of the human accounts both fake and real had their pictures and name on it.

After our research we find that those accounts which are real had on an average more than 30 follower. So, we must discard those

accounts which have more than 30 followers.

When we do so we must create at least ten-twenty thousand fake accounts so that we have enough data so that our algorithm may recognise what a fake account really is and all the accounts must be created by humans not by bots.

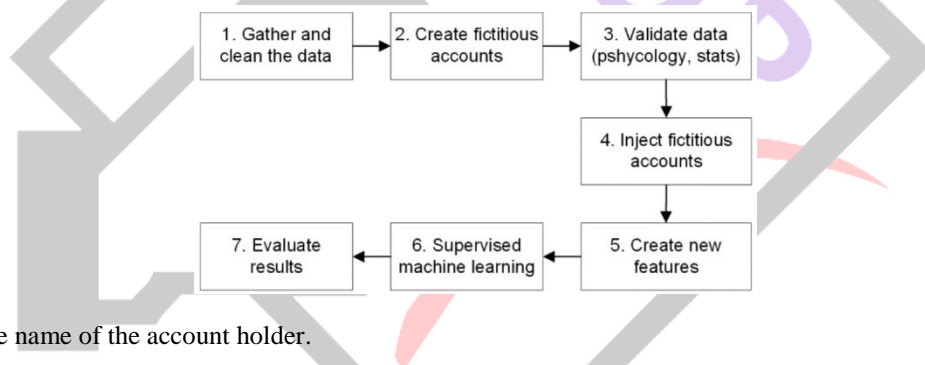
After reading about research in psychology, we concluded that in most of the fake accounts people mostly lied on their ages for instance mostly people set the age as 18-19 so that they make their account eligible for creation, people also lie about their gender, the images are also mostly downloaded from internet and some accounts have image of a character of different gender as set in their gender section by them. The locations of the accounts are mostly different as they do not want to be tracked, but mostly they lie about their names for instance there are several accounts of Dwayne Johnson on twitter, facebook, Instagram such as 'Dwayne the rock official', 'TheRockOfficial' etc.

Following are the features used to build a profile:

- 1) Name of the account.
- 2) Description of the profile.
- 3) Number of follower.
- 4) Number of friends.
- 5) Account created at.
- 6) Tweets.
- 7) Profile Pictures.

III. METHODOLOGY

Our system focuses on a set of tweets to build a user behavioral profile. A behavioral profile contains all tweets posted by a user and other things which are required to post the tweet like Name of account, Number of followers, etc. Once our system obtains the set of messages for each user, this information is used for building behavioral profile. Then system extracts feature values from each tweet and for each feature, feature model is trained. On the basis of a behavioral profile, we can determine to what extent a new message follows the expected behavior. Each profile data obtains feature value between $[0, 1]$, where "1" shows genuine account and "0" shows probably the fake account. After computing anomaly score for each feature, we have to calculate anomaly score for the whole message. To detect the genuine and fake accounts we have to combine all feature value scores of a message.



1. NAME: The name of the account holder.
2. DESCRIPTION: The bio of the profile.
3. NUMBER OF FOLLOWER: The number of follower the account has.
4. NUMBER OF FRIENDS: The number of friends the account follows.
5. CREATED AT: The time when the account was created.
6. TWEETS: The tweets made by the account.
7. PROFILE PICTURES: The image which is set up by the account.

With SOCIAL MEDIA PLATFORMSs, the data character of the accounts, the relations between record and others and lastly the record's behaviour and messages. To distinguish counterfeit fake bot accounts in SOCIAL MEDIA PLATFORMSs, there are combinations developed by connecting various engineered features to machine learning models. A model is given in which a lightweight preparation show in view of the personality of the record is given by Cresci et al. Cresci et al in their model shows that the characteristic features of the record is adequate to distinguish the record between the normal or bots. Gupta et al. conducted and planned, the recurrence and types of messages and on what particular time of day, gives more data pertinent to sneakiness than the characteristics features of the record itself. Distinguishing the conduct during opinion was likewise effective for particular item of enthusiasm, for instance races. By the outcomes shown by Cresci et al. we proposition in order to likewise utilize comparative Lightweight Classifier that exclusively incorporates information portraying the character of a record.

IV. CONCLUSION

In the end, we conclude that the research work have been done to detect, identify and eliminate fake bot accounts created and cyborgs cannot be used for differentiating fake account created by human beings. As machine learning has evolved in recent days. We can differentiate fake accounts easily by applying a data set with fake accounts and marking them as fake and real accounts marking them as real. So, after the model knows which account fake and which account is real, the model will be successfully able to differentiate a fake account created by human from a real one when the actual data set will be given to it.

V. ACKNOWLEDGMENT

This work is based on data collected as part of the project “ Fake Followers Detection On Twitter” by Bachelor of Engineering students of Shree L.R Tiwari College of Engineering, under the supervision of Prof. Sunil Yadav, Department of Information Technology, Shree L.R Tiwari College of Engineering, Thane, Maharashtra.

REFERENCES

- [1] Pooja V. Phad, Mr. M. K. Chavan (2017). “Detecting Compromised High-Profile Accounts on Social Network.
- [2] Savvas Zinonos, Andreas Tsirtsis and Nicolas Tsapatsoulis, Mallidi Sarredd, and Sanjay Singh(2018). “Twitter Influencers or Cheated Buyers.
- [3] Reema Aswani & Arpan Kumar Kar1 & P. Vigneswara Ilavarasan(2018). “Detection of Spammers in Twitter marketing: A Hybrid Approach Using Social Media Analytics and Bio Inspired Computing”.
- [4] ESTÉE VAN DER WALT and JAN ELOFF(2018). “Using Machine Learning to Detect Fake Identities: Bots vs Humans ,”.
- [5] Ashish Mehrotra, Mallidi Sarredd, and Sanjay Singh(2016). “Detection of Fake Twitter Followers using Graph Centrality Measures.
- [6] Naman Singh, Tushar Sharma , Abha Thakral, tanupriya Choudhury(2018.). “Detection of Fake Profile in Online Social Networks Using Machine Learning.
- [7] Neil Shah*, Hemank Lamba*, Alex Beutel†, Christos Faloutsos(2017) “The Many Faces of Link Fraud

