Title: Bot Detection in Social Media Accounts

Name: Aayush Tyagi
Roll Number: 2013206 (A-03)
Semester: 4th sem, B.Tech(Core)
Email: tyagiaayush5@gmail.com

Problem Statement: 2.

Bot Detection in Social Media Accounts: In social media (Facebook, twitter, Instagram) there are multiple bot accounts used by various political parties or organization for their benefits. Can you develop an algorithm to detect the bot accounts using some of the properties/features of bot accounts? It will help to us to use the data from real accounts in multiple analysis.

Motivation:

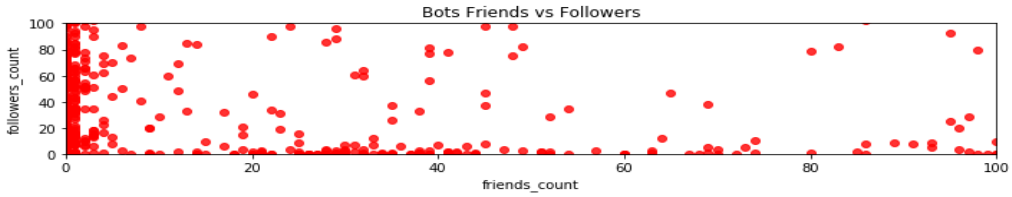
Twitter bot is used to produce automated posts, follow Twitter users or serve as spam to entice clicks on the Twitter micro blogging service. Twitter is an online news and social networking service where users post and interact with messages, "tweets" restricted to 140 characters. There are 310M monthly active twitter users and a total of 1.3 billion accounts have been created and 500M tweets per day. Since it's such an influential platform people have developed Twitter bots. These bots are used to increase number of followers, retweeting, spamming etc. and there are about 48M bots today. This problem is mostly faced by common users. These include directing more visitors to certain websites which can be considered as spam, influence a community on a specific topic, spread misinformation, recruit people to illegal organizations, manipulating people for stock market actions, and blackmailing people to spread their private information by the power of these accounts.
Consequently, social bot detection is of great importance to keep people safe from these harmful effects.

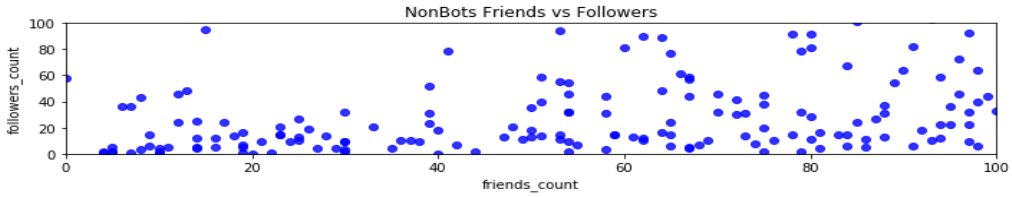
How can we detect a bot?

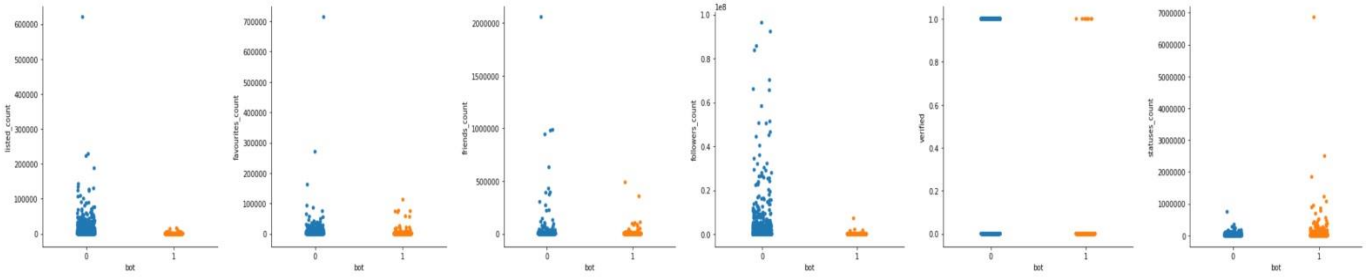
Now you know what a bot is, but the bigger question is would you know a bot if you encountered one? Depending on the level of stealth employed by a bot, some are easier to detect than others.

Some typical characteristics of bots on Twitter include:

- Many Twitter bots have a relatively recent creation date.
- Many bot user names contain numbers, which can indicate automatic name generation.
- The account primarily retweets content, rather than tweeting original content.
- The account's tweet frequency is higher than a human user could feasibly achieve.
- The account may have a high number of followers and also be following a lot of accounts; conversely, some bot accounts are identifiable because they send a lot of tweets but only have a few followers.
- Many bots tweet the same content as other users at roughly the same time.
- Short replies to other tweets can also indicate automated behavior.
- There is often no biography, or indeed a photo, associated with bot Twitter accounts.







Proposed Solution-

- Understand psychology behind bot creation
- Implement different machine learning algorithms
- Hashing technique to quickly organize the user accounts in clusters of abnormally correlated accounts
- Custom classification algorithm
- Do not consider Attributes like id, status_count, default_profile, image etc. there should be no correlation between them
- Consider attributes like followers,friends, verified account etc.
- Other attributes like name, description, status for feature extraction.
- Existing solutions use naive bayes and decision trees
- We are planning to implement our own custom algorithm based on few feature extraction
- Aiming to get highest accuracy and differentiate between real twitter accounts and bots

Methodology:

Types Of Attributes

1)Integers: ID, Friends ,Followers, Favorites, Statuses, listed count(tagging people)

2) String: Name, Location ,Description ,URL, Language

3)Boolean: Verified Account, Default Profile

4)Date: CreatedAt

Other Derived attributes like age, account has name bot in it.

Requirements:

- numpy
- Python3
- pandas

- matplotlib
- sklearn

After data analysis we implemented 4 algorithms:

1. KNN
2. SVM
3. Multinomial Naive Bayes
4. Random Forest
5. Decision Tree
6. Custom Classification Algorithm

Custom classification algorithm which is basically my own algorithm.

PROCESS:

Step 1: Clean the Data and prepare it to do Classification. Make a function to check Performance of the classifiers.

Step 2: Consider the attributes which determine a twitter account to be a bot or non bot.

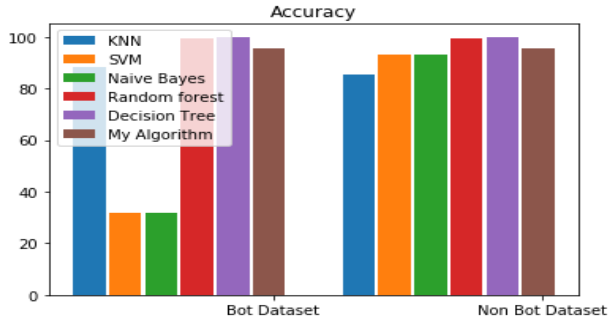
Step 3: Create a bot identification criteria based on attributes and classify the dataset randomly into train and test dataset.

Step 4: Apply Different classification method and find accuracy of each method.

Step 5: After the classification is completed Compare Accuracy of Different methods and find the most relevant one.

Step 6: Work on Test data and find the Result by the best found classifier and store it.

Result: Accuracy of all method has been compared and the best method is found to be Decision Tree. Worked on test data using Decision tree and store result in Result.csv



Future Work: In the future, we can implement a Web service (for example, an API) to allow the research community to perform tweet-level bot detection using it.