FINAL YEAR PROJECT

Preliminary Report

Author:
Marcell BATTA

Supervisor:
Dr. Lahcen OUARBYA

A thesis submitted in fulfilment of the requirements
for BSc Computer Science Degree

February 12, 2019

Contents

Tweet The name for a message on Twitter with a limit of 280 characters.

description

Chapter 1

Introduction

Social media has become an integral part of our lives in the past years as we spend more time online than ever before. Roughly 30% of our online time is spent on social media interactions, Twitter being one of them. Twitter is arguably the largest source of news on the internet. This is due to the nature of information spreading on the platform through tweets and retweets. At this point, because of the scale, it is impossible to monitor it all to make sure everything is accurate and that there is no false propaganda being spread.

1.1 Aim

The aim of this project is to create a program with an underlying algorithm that will attempt to figure out whether a Twitter account is under the control of a human or is purely being controlled by a script that someone wrote. The issue doesn't come from there being accounts not directly used by people or 'bots', instead from the ones that claim to be real individuals when they in fact are not. With the use of a program such as this, it is possible to see trends in current events and point out patterns in how the network of these bots are run and what they are targeting exactly.

Chapter 2

Background Research

This chapter contains the information found before beginning development of the program, along with some systems that are already available and a summary on them.

2.1 Politics

Politics is probably the biggest concern when it comes to these bot accounts. They are the reason why false information spreads so fast. This is because of the way Twitter works with its trending hashtags. These bots will tweet and retweet about important and most likely incorrect matters, they also make use of popular hashtags that basically define the topic of a tweet. This then leads to these malicious tags to become trending for everyone to see.

2.1.1 2016 US Elections

The 2016 elections in America was one of the, if not the biggest outburst of Twitter bots we have yet to see. It was found that by extrapolating some findings, roughly 19 percent of 20 million election related tweets originated from bots between September and October of 2016. According to the same study it was also found that around 15 percent of all accounts that were involved in election related tweets were bots. Now even though that is a lot of attention for these tweets containing false information, they will mostly only be seen by people who are already on the same side and agree. However, this doesn't rule out the affects. A study by the NBER(National Bureau of Economic Research) came to the conclusion that these bots were the cause of up to 3.23 percent of the votes that went towards Donald Trump. This tells us that even if it's just marginal, it does still affect the outcomes.

The interesting part of all this is that the bots immediately went silent and disappeared as the election ended. The accounts though didn't get deleted but they simply went into hibernation waiting for their next bit of propaganda that needed to be spread. In 2017, 2000 of these bots reemerged to take part in the French and German elections as well, meaning they were run by the same people. They were discovered to make up for 1 in 5 election related tweets.

2.1.2 2018 US Mid-Term Election

2.2 Existing Systems

There is a handful of algorithms or programs that have been designed to detect these bots.

2.2.1 Tweetbotornot

Tweetbotornot is a package built in R that uses machine learning to classify Twitter accounts. It has two 'levels'. One for users where it uses information related to an account such as location or number of followers. The other is a tweet-level which checks for details like hashtags, mentions or capital letters out of the user's more recent 100 tweets. This could prove useful when testing my program to compare results as the accuracy of this library is 93.8 percent. As this is just a package created, it doesn't have any user-interface program built around it or anything like that, therefore is unusable by anyone not knowledgable in R.

Chapter 3

System Design

3.1 Method

The core part of the system will be deciding whether the account it is checking is a bot or not. It will use a form of machine learning to classify the account as either 'bot' or 'not bot'. Initially it would seem as if this was a binary classification issue, however it makes more sense to treat it as a regression problem. This makes it much easier to interpret the results for the user as a probability is easily understood and is a much more honest answer compared to just giving the user a 'yes' or 'no'.

3.2 System Requirements

In order to achieve the aims of the system, there are a few things the program will need to do.

1. The system must be able to determine whether an account is a bot or not.
2. A connection using the Twitter API must be established in order to retrieve users' data.
3. Allow users to input a Twitter account.
4. Display the likelihood that an account is a bot or not.

Chapter 4

Planning

Appendix A

if appropriate