Data Mining
Identification and classification of Twitter Bots

Github Account

Joaquin Quintana

Jason Weidner

Description

Bots are ubiquitous on social media platforms and researchers have developed many techniques to identify bots and bot swarms. We aim to use open source Twitter data, gathered by academic researchers, to see if we can successfully identifying bots using clustering or decision trees.

The particular dataset we've downloaded was generated to identify so called 'social spambots', recent bots used on Twitter developed to evade detection. Social spambots often tweet normal content but also work in highly coordinated fashion to promote specific content (like promoting the tweets of specific politicians during an election campaign).

Prior Work - 1

Cresci, Di Pietro, Petrocchi, Spognardi, and Tesconi. 2017. *The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race.* In Proceedings of the 26th International Conference on World Wide Web Companion (WWW '17 Companion). International World Wide Web Conferences Steering Committee Link

- Claims new bot technology evades state of the art academic bot identification techniques. People can't ID bots either.

Cresci, Di Pietro, Petrocchi, Spognardi and Tesconi, "Social Fingerprinting: Detection of Spambot Groups Through DNA-Inspired Behavioral Modeling," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 561-576, 1 July-Aug. 2018. Link

- Creates 'digital DNA' for each Twitter account by translating activity to letters (e.g. ATCGXN) and compares sequences to those from known bots and authentic accounts. This technique can identify new generate 'social spambots' that have evaded detection otherwise.

Cresci, Di Pietro, Petrocchi, Spognardi and Tesconi. Fame for sale: Efficient detection of fake Twitter followers, Decision Support Systems, Volume 80, 2015, Pages 56-71, ISSN 0167-9236. Link

- Created datasets of bot and authentic accounts and scraped their data. Authentic were verified by sociologists and CAPTCHA. Bots were purchased. Evaluates categorisation techniques using dataset based on academic and media proposed rules. Media rules performed poorly. Academic rules did quite well.

Prior Work - 2

Besko and Carley. 2020. *TBot-Match: Social Bot Detection with Recursive Nearest Neighbors Search.* Link

- Shows a semi-supervised approach to identifying bots based on network and tweet semantic data. Embedding the network and semantic data takes ~2 days so is impractical for our use.

Chavolshi, Hamooni and Mueen. Identifying Correlated Bots in Twitter. Social Informatics, 8th Intern'l Conference, Bellevue, WA, USA, Nov 2016 Part II, pp. 14-21. Link

Cresci. *A Decade of Social Bot Detection*. Commun. ACM 1, 1 (July 2020), 16 pages. https://doi.org/10.1145 Link

Guo, Cho, Chen, Sengupta, Hong and Mitra. *Online Social Deception and Its Countermeasures: A Survey*. journal article here.

Datasets

Dataset acquired from Github Bot Repository from Botometer

Download dataset from Bot Repository:
https://botometer.osome.iu.edu/bot-repository/datasets/cresci-2017/cresci-2017.csv.zip

Dataset has been downloaded to each user's personal machine. Code for the project is being placed in a Jupyter notebook and changes are being tracked via a github collaboration.

Summary of Dataset (Cresci 2017)

		statistics		
dataset	**description**	accounts	tweets	year
`genuine accounts`	verified accounts that are human-operated	3,474	8,377,522	2011
`social spambots #1`	retweeters of an Italian political candidate	991	1,610,176	2012
`social spambots #2`	spammers of paid apps for mobile devices	3,457	428,542	2014
`social spambots #3`	spammers of products on sale at *Amazon.com*	464	1,418,626	2011
`traditional spambots #1`	training set of spammers used by Yang *et al.* in [43]	1,000	145,094	2009
`traditional spambots #2`	spammers of scam URLs	100	74,957	2014
`traditional spambots #3`	automated accounts spamming job offers	433	5,794,931	2013
`traditional spambots #4`	another group of automated accounts spamming job offers	1,128	133,311	2009
`fake followers`	simple accounts that inflate the number of followers of another account	3,351	196,027	2012
`test set #1`	mixed set of 50% `genuine accounts` + 50% `social spambots #1`	1,982	4,061,598	–
`test set #2`	mixed set of 50% `genuine accounts` + 50% `social spambots #3`	928	2,628,181	–

Table 1: Statistics about the datasets used for this study.

The paradigm-shift of social spambots

Evidence, theories, and tools for the arms race

Stefano Cresci [†] s.cresci@iit.cnr.it
Roberto Di Pietro [†‡§] roberto.di_pietro@nokia.com
Marinella Petrocchi [†] m.petrocchi@iit.cnr.it
Angelo Spognardi [†¶] angsp@dtu.dk
Maurizio Tesconi [†] m.tesconi@iit.cnr.it

[†] Institute for Informatics and Telematics, IIT-CNR, Pisa, Italy
[‡] Nokia Bell Labs, Paris, France
[§] Department of Mathematics, University of Padua, Padua, Italy
[¶] DTU Compute, Technical University of Denmark, Denmark

Proposed work:

- **Data cleaning**
  - Removing non-English content
  - Reducing size for ease of processing
  - Identifying Nan, no values and replacing them appropriately

- **Data preprocessing**
  - Split data: train/test
  - Possibly precalculate bag of words for each account
  - Possibly create directed graph for each account, pruning nodes not present in the dataset

- **Data integration**
  - Unlikely, as the data is already labeled (bot/authentic)
  - Unlikely, because the data already includes tweets, followers and metadata

List of tools (intended to be used)

- Python/Jupyter notebook
- git/github
- Pandas
- Matplotlib
- Possibly numpy (for statistical analyses)
- Possibly seaborn (for visualisation)

Evaluation

Attempt to reproduce some legacy analyses

- Determine if information gain and decision trees can be used to identify the most important attributes to identify traditional and/or social spambots.
- Determine if clustering can be used to identify traditional or social spambots meaningfully.
- Our dataset includes both traditional bots, social spambots and authentic twitter account data.

Key article:

Cresci, Di Pietro, Petrocchi, Spognardi and Tesconi. Fame for sale: Efficient detection of fake Twitter followers, Decision Support Systems, Volume 80, 2015, Pages 56-71, ISSN 0167-9236. Link