Social Bots Detection on Twitter

Authors:

1. Qiwei Zhou, New York University Tandon School of Engineering, Brooklyn, New York, qz729@nyu.edu
2. Jiao Wu, New York University Tandon School of Engineering, Brooklyn, New York, jw4321@nyu.edu
3. Introduction

As the popularity of social networking and microblogging tools continues to grow, accounts controlled by automated programs, known as social bots (or bots for short), have risen from the horizon. Twitter, with the openness of its platform and API, has seen the rise of the machines. These bots automatically produce contents and even communicate with humans, trying to hide themselves among the mass population of Twitter. In this project, we are going to compare the performance of two different machine learning algorithms for detecting bot accounts.

1. Motivation

Although plenty of bots on Twitter are benign, there are still bad bots that mislead, exploit and manipulate online conversations with rumors, spam, phishing links and slander [1]. These bots randomly add other users as their friends and if the user follows back, the malicious contents will be displayed on his homepage [2]. They can also be alleged to help political candidates in the election [3], potentially undermining the democratic system. Therefore, we need to develop a method to detect these bots in social media, either to help Twitter manage the community [4], or to help human users identify who they are communicating with.

1. Related Work

[1] Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. 2015. The Rise of Social Bots. X, X, Article XX ( 201X), 11 pages.

[2] Z. Chu, S. Gianvecchio, H. Wang and S. Jajodia, "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811-824, Nov.-Dec. 2012. doi: 10.1109/TDSC.2012.75

[3] J. P. Dickerson, V. Kagan and V. S. Subrahmanian, "Using sentiment to detect bots on Twitter: Are humans more opinionated than bots?," 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), Beijing, 2014, pp. 620-627.

[4] N. Chavoshi, H. Hamooni and A. Mueen, "DeBot: Twitter Bot Detection via Warped Correlation," 2016 IEEE 16th International Conference on Data Mining (ICDM), Barcelona, 2016, pp. 817-822.

[5] Bot or Not: an end-to-end data analysis in Python, Erin Shellman. Available: http://www.erinshellman.com/bot-or-not/

1. Data.

In this project, we collected 100 twitter user information. Since twitter has released a set of API functions that support user information collection, we used REST APIs to retrieve our required user information, ranging from profile, follower, friend lists, status etc., For each user, we called GET users/lookup method to collect user information and could get up to 100 users per request. Thus, this method is very efficient for getting the details of such many users. To test the performance of two different algorithms for detecting bot account, we collected 100 twitter users, half of them are bot and the others are not bot. Here we used bot twitter accounts that had been clearly identified and not bot accounts from twitter social network. Based on the previous observations of differences among human and bot accounts [3], we selected 20 data fields for each of the 100 users for future analysis. The details of dataset are saved as a CSV file for following parts of this project.

1. Algorithms plan to use

We are going to use Naïve Bayes, Random Forest [5] for this project.