8-2019

Structural Bot Detection in Social Networks

Lale Madahali

Structural Bot Detection in Social Networks

LALE MADAHALI, University of Nebraska at Omaha, United States

Social network platforms are a major part of toady's life. They are usually used for entertainment, news, advertisements, and branding for businesses and individuals alike. However, use of automated accounts, also known as bots, pollute this environment and avoid having a reliable clean online world. In this work, I address the problem of detecting bots in online social networks.

Additional Key Words and Phrases: social bots, social networks analysis, graph analysis

ACM Reference Format:
Lale Madahali. 2019. Structural Bot Detection in Social Networks. 1, 1 (August 2019), 4 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Web 2.0 social networks has made bots rise increasingly on different new platforms. There are different typologies of bots available including Webrobots, chatbots, spambots, sockpuppets and trolls, cyborgs and hybrid accounts, and social bots [13]. Webrobots also known as crawlers and scrapers were used to download and index websites. And, finally, they are a major part of search engines [21] [22]. Chatbots are built to interact with humans directly through natural language via text or speech. Spambots have been there even before the inception of the Internet on bulletin boards like USENET. Spambots are computers or other networked devices compromised by malware and controlled by a third party. Many of spambots working together to attack large networks can perform Distributed Denial of Service (DDoS) attacks. Sockpuppets are fake identities that interact with ordinary users on social networks [4]. The name sockpuppet means manual control over accounts, but it is also used to include automated bot accounts [2]. Trolls are sockpuppets created for political goals, or coordinated by government proxies or interrelated actors. Cyborgs are bot-assisted human or human-assisted bot. Hybrid accounts are people who willingly give their real profiles to be automated for political purposes. So far, the exact difference between social bots, cyborgs, and sockpuppets is not obvious owing to the background theories and level of their automation [8]. Social bots exist in various platforms. In Wikipedia, bots help with editing and vandalism detection. Twitter has an open Application Programming Interface (API) allowing developers to deploy automation through third party applications and tools [6]. Some types of social bots fabricate an identity and infiltrate real networks of users. These bots are called "sybils". The name "sybil" is an information security term and is refered to an actor that controls multiple false nodes within a network [3]. In this study, I investigate the problem of detecting social bots through their structural basis (i.e. how they form) and their dynamic activities.

Author's address: Lale Madahali, University of Nebraska at Omaha, Omaha, Nebraska, United States, lmadahali@unomaha.edu.

XXXX-XXXX/2019/8-ART $15.00
https://doi.org/10.1145/1122445.1122456

2 RELATED WORK

As per my observation and knowledge, research on bots is new and immature. The first paper on social bots was published in 2011, which was about automated accounts that infiltrated real networks of users and spread malicious links or advertisements [3]. Bots can be found on different platforms like Wikipedia and Twitter. The difference in the structure of existing platforms lead to different functionalities and applications for bots. Wikipedia bots work as guardians and help in editing and avoiding vandalism. Bots are known in Wikipedia by their names and they have policies and rules [14]. Twitter bots are generally not distinguishable and, therefore, they are not easily detectable. This can bring about challenges such as influence campaigns can leverage bots to spread their thoughts and news and individuals will get deceived and may lose their valuable information. One of the major subcategory of social bots are political bots [15]. Political bots were used for the first time during the 2010 Massachusetts Special Election in the United States in which a small network of automated accounts were used to create a campaign against one of the candidates [17]. Researchers found that social bots have also been used to distort the political mobilization in Syria [1] [26] and Mexico [25]. Social bots can be used for beneficial purposes such as search engine optimization as well [23].

3 RESEARCH PLAN

This work tries to address the challenge of detecting automated accounts known as social bots on Twitter. The project will be divided into four steps.

First, I will examine whether the network ties between bots are social networks or information network. We need to define the social network and an information network to answer this question. In this respect, there are many definitions of a social network. However, here we characterize a social network by having degree assortativity, small shortest path lengths, large connected components, high clustering coefficients, and a high degree of reciprocity. We define an information network as a structure in which the main goal is content dissemination, leading to/imposing large vertex degrees, lack of reciprocity, and large two-hop neighborhoods. The importance of knowing the structure of bots' networks is that it clarifies how these networks arise and evolve. it is worthwhile to know because bots are contributing in social media and knowing them more help us to identify, classify, and understand their purposes more.

Second, I try to recognize the graphical attributes of bots' activities, dynamics, and their network formation models. Examining how they interact with each other and other individuals can help detect them better. More importantly, I am investigating how they form their network ties and study whether it is similar to real people. Understanding bots' network models contribute to understanding their ties and structures.

Third, I am interested in understanding how adhering to fraudulent laws can help with detecting bots. In other words, knowing whether they follow the laws such as Benford's Law is valuable in that I understand their attributes better. According to Benford's Law in normal activities on social networks 30% of the time numbers begin with a one (1) and they are likely to happen six times more than numbers beginning with a nine (9) [12]. This law has many applications in naturally-occurring systems like natural sciences [24], stock market [9], validating survey data [16], and religions [19]. It is used as an auditing tool in digital forensics areas like financing [7], accounting [10]. I am interested in finding out whether automated accounts follow naturally-occurring laws and show the same pattern or they deviate and can be detectable through applying these laws.

Finally, I will investigate which social influence theories are applicable to social influence bots networks. I will try to test these theories on social influence bots. This will help advancing the theories in this realm.

In order to accomplish the above steps, I will use benchmark datasets. I will try to use supervised and unsupervised techniques and therefore, I use datasets with known bots and unknown bots. I will use datasets in [20] and [11] for supervised learning and Twitter Election Integrity datasets[1] for unsupervised part of the project. These robust datasets contain millions of tweets that are promising in identifying and analysis social bots and their characteristics. I will also consider creating an algorithm to detect bots and compare it with existing platforms like Debot [5], Botwalk [18], BotOrNot [8], and Botometer.

REFERENCES

[1] Norah Abokhodair, Daisy Yoo, and David W McDonald. 2015. Dissecting a social botnet: Growth, content and influence in Twitter. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 839–851.

[2] Marco T Bastos and Dan Mercea. 2019. The Brexit botnet and user-generated hyperpartisan news. *Social Science Computer Review* 37, 1 (2019), 38–54.

[3] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. 2011. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th annual computer security applications conference*. ACM, 93–102.

[4] Zhan Bu, Zhengyou Xia, and Jiandong Wang. 2013. A sock puppet detection algorithm on virtual spaces. *Knowledge-Based Systems* 37 (2013), 366–377.

[5] Nikan Chavoshi, Hossein Hamooni, and Abdullah Mueen. 2016. DeBot: Twitter Bot Detection via Warped Correlation.. In *ICDM*. 817–822.

[6] Zi Chu, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. 2010. Who is tweeting on Twitter: human, bot, or cyborg?. In *Proceedings of the 26th annual computer security applications conference*. ACM, 21–30.

[7] Paulette Clippe and Marcel Ausloos. 2012. BenfordâĂŹs law and Theil transform of financial data. *Physica A: Statistical Mechanics and its Applications* 391, 24 (2012), 6556–6567.

[8] Clayton Allen Davis, Onur Varol, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer. 2016. Botornot: A system to evaluate social bots. In *Proceedings of the 25th International Conference Companion on World Wide Web*. International World Wide Web Conferences Steering Committee, 273–274.

[9] Marc JK De Ceuster, Geert Dhaene, and Tom Schatteman. 1998. On the hypothesis of psychological barriers in stock markets and Benford's Law. *Journal of Empirical Finance* 5, 3 (1998), 263–279.

[10] Cindy Durtschi, William Hillison, and Carl Pacini. 2004. The effective use of BenfordâĂŹs law to assist in detecting fraud in accounting data. *Journal of forensic accounting* 5, 1 (2004), 17–34.

[11] Zafar Gilani, Reza Farahbakhsh, Gareth Tyson, Liang Wang, and Jon Crowcroft. 2017. Of Bots and Humans (on Twitter). In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (ASONAM '17)*. ACM, New York, NY, USA, 349–354. https://doi.org/10.1145/3110025.3110090

[12] Jennifer Golbeck. 2015. BenfordâĂŹs law applies to online social networks. *PloS one* 10, 8 (2015), e0135169.

[13] Robert Gorwa and Douglas Guilbeault. 2018. Unpacking the social media bot: A typology to guide research and policy. *Policy & Internet* (2018).

[14] Aaron Halfaker and John Riedl. 2012. Bots and cyborgs: Wikipedia's immune system. *Computer* 45, 3 (2012), 79–82.

[15] Philipp N Howard and SC Woolley. 2016. Political communication, computational propaganda, and autonomous agents-Introduction. *International Journal of Communication* 10, 2016 (2016).

[16] George Judge and Laura Schechter. 2009. Detecting problems in survey data using BenfordâĂŹs Law. *Journal of Human Resources* 44, 1 (2009), 1–24.

[17] Panagiotis T Metaxas and Eni Mustafaraj. 2012. Social media and the elections. *Science* 338, 6106 (2012), 472–473.

[18] Amanda Minnich, Nikan Chavoshi, Danai Koutra, and Abdullah Mueen. 2017. BotWalk: Efficient adaptive exploration of Twitter bot networks. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*. ACM, 467–474.

[19] TA Mir. 2012. The law of the leading digits and the world religions. *Physica A: Statistical Mechanics and its Applications* 391, 3 (2012), 792–798.

[20] Fred Morstatter, Liang Wu, Tahora H Nazer, Kathleen M Carley, and Huan Liu. 2016. A new approach to bot detection: striking the balance between precision and recall. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 533–540.

[21] Christopher Olston, Marc Najork, et al. 2010. Web crawling. *Foundations and Trends® in Information Retrieval* 4, 3 (2010), 175–246.

[22] Gautam Pant, Padmini Srinivasan, and Filippo Menczer. 2004. Crawling the web. In *Web Dynamics*. Springer, 153–177.

[1]https://about.twitter.com/en$_{u}s/values/elections - integrity.htmldata$

[23] Jacob Ratkiewicz, Michael Conover, Mark Meiss, Bruno Gonçalves, Snehal Patil, Alessandro Flammini, and Filippo Menczer. 2011. Truthy: mapping the spread of astroturf in microblog streams. In *Proceedings of the 20th international conference companion on World wide web*. ACM, 249–252.

[24] Malcolm Sambridge, Hrvoje Tkalčić, and A Jackson. 2010. Benford's law in the natural sciences. *Geophysical research letters* 37, 22 (2010).

[25] Pablo Suárez-Serrato, Margaret E Roberts, Clayton Davis, and Filippo Menczer. 2016. On the influence of social bots in online protests. In *International Conference on Social Informatics*. Springer, 269–278.

[26] John-Paul Verkamp and Minaxi Gupta. 2013. Five incidents, one theme: Twitter spam as a weapon to drown voices of protest. In *Presented as part of the 3rd {USENIX} Workshop on Free and Open Communications on the Internet*.