9-2020

# Bots and Humans on Social Media

Lale Madahali

# Bots and Humans on Social Media

**Lale Madahali**
lmadahali@unomaha.edu
University of Nebraska at Omaha

## ABSTRACT

Social networks are an important part of today's life. They are used for entertainment, getting the news, advertisements, and branding for businesses and individuals alike. Research shows that automated accounts, also known as bots, contribute to the content spread on social media allowing the the environment pollution and public opinion manipulation. This research aims at investigating bots' behavior on Twitter and examine how different and similar they are compared to humans. I will investigate their underlying network, whether it is an information network or social network. In the second step, I attempt to answer whether they follow the structure of scale-free networks. In the third step, their conformity to the law of naturally-occurring systems. Finally, I study their graphical attributes and perform a comparative analysis with other existing algorithms and platforms. This research gives insights into the better understanding of behavior of bots and their activities leading to bot detection improvement.

## KEYWORDS

social networks, social bots, graph analysis

**ACM Reference Format:**
Lale Madahali. 2020. Bots and Humans on Social Media. In *Proceedings of Tapia '20: ACM Richard Tapia (Tapia '20).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/1122445.1122456

## 1 INTRODUCTION

Social networks make the world smaller. It makes news dissemination and communication faster. However, all technologies have their own demerits and bring about challenges. Using social media to influence public opinion is a growing trend. The reason is that businesses use social media as a podium to introduce their services and products, politicians and celebrities use social media to build their public image, and people are exposed to a huge volume of data.

Social bots are automated accounts running on social media. Cyborgs are another type of human-assisted automated accounts. Not all social bots are malicious [1]. However, the fact that they impersonate themselves and misrepresent their identity makes them "unwanted minions". Their unknown identity can lead to unexpected or malicious operations. Therefore, there is a need for detecting and understanding them.

Social networks have made the world smaller and people closer to each other. Services like Twitter, Facebook, and Instagram have provided a ubiquitous service to connect people. There are studies showing different characteristics of humans and bots in terms of tweeting, replying, and befriending people [5] [6]. Some studies explored bot detection and improvement of machine learning algorithms for detection of bots [7][8], and a huge body of research is dedicated to use of bots on public opinion manipulation [9][10][11]. However, there is still lack of knowledge about the structure of bots' networks. Knowing the bots' underlying structure helps in better understanding of bots, improvement of their detection, and defining the nature of their activities. It also contributes to the field of cyber security such that social bots play a major role in spreading misinformation and manipulating public opinion.

In this work, I will investigate the graphical underlying structure of bots' activities to gain insights into the nature of bots and their activities that helps improve their detection. It also contributes to the field of cyber security since social bots play a major role in spreading misinformation and manipulating public opinion. To this end, first I investigate whether their underlying network is an information network or social network. In the second step, I attempt to answer whether they follow the structure of scale-free networks. In the third step, I will test if their activities deviate from the law of naturally-occurring system. Finally, I study their graphical attributes and perform a comparative analysis with other existing algorithms and platforms [2][4].

## 2 RELATED WORK

Despite the fact that the fake news detection and platforms is grown widely, the research in social bots is not very mature. The first paper published on social bots was in 2011 by Boshmaf regarding the infiltration of social networks by social

*Tapia '20, September 16–19, 2020, Dallas, TX*

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

bots [12]. According to Adewole and colleagues [2], the majority of research in social bots is on machine learning (68%), 28% used graph techniques, and only 4% focused on crowd sourcing. Many papers on machine learning use supervised machine learning including Naïve Bayes [13], Meta-based [14], SVM [15], and Neural Network [20]. However, unsupervised machine learning has been used including hierarchical [15], partitional [17], PCA-based [16], Stream-based [18], and correlated pairwise similarity [2].

Additionally, a huge body of literature in this area is on use of social bots in public opinion manipulation and elections. One of the major subcategories of social bots are political bots [19]. 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 was used to create a campaign against one of the candidates [20]. Researchers found that social bots have also been used to distort the political mobilization in Syria [21] [22] and Mexico [23].

## 3 RESEARCH PLAN

This work tries to investigate the underlying structure of social bots' networks in four steps. First, I will examine whether the network ties between bots follow the structure of social networks or information networks. This clarifies how bots' underlying network arises and evolves, which in turn helps us better identify, classify, and understand their purposes. To this end, we first need to define the social network and information network. Although there are many definitions of a social network, here we characterize a social network by having degree assortativity, small shortest path lengths, large connected components, high clustering coefficients, and high degree of reciprocity. We also define an information network as a structure in which the main goal is content dissemination, leading to large vertex degrees, lack of reciprocity, and large two-hop neighborhoods [24] [25]. Therefore, we try to answer this question, "Is bots' network a social network or an information network?".

Second, the topology of bots' follower networks is of great importance. The topology of large complex networks falls into three categories: random, small-world, and scale-free. Three network statistics are used to determine their topology: average path length, average clustering coefficient, and degree distribution [26]. Adhering to scale-free structure is another contributing determinant of real-world networks. We will examine the bots' networks statistics to see their underlying structure by measuring the goodness-of-fit of the network statistics. To test the scale free structure, we will look at the degree distributions and their power-tail shape and utilize the Clauset test [27]. In this test, the null hypothesis is that the distribution is power-tailed, and the alternative hypothesis is a non-power-law distribution, leading to this question, "Is bots' networks a scale-free network?".

Third, we will examine how adhering to fraudulent laws can help with detecting bots. In other words, knowing whether they follow the laws of digital fraud such as Benford's Law is valuable to better understand their attributes. 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 [28]. This law has many applications in naturally-occurring systems like natural sciences [29], stock market [3], validating survey data [30], and religions [31]. It is used as an auditing tool in digital forensics areas like financing [32], and accounting [33]. We are 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, we will run machine learning algorithms to see the performance of graphical features in determining bots. Features will include in-degree, out-degree, clustering coefficient, pagerank, propflow, jaccard coefficient, and Katz [36]. Then, we will compare the performance of running algorithms with existing work [7] [2] [34][1].

## 4 DATA

To achieve the goals mentioned, a follower (or communication) graph of humans and bots is needed. Because calculating the graphical features needs a collective connection of bots and humans, we need to scrape Twitter over trending topics. Then, the data need to be annotated by existing tools like Debot [2], BotorNot [4], Botometer, using R package tweetbobornot, using Benford's law and also qualitatively to ensure the quality. Once the annotated graph is ready, we can extract the graphical features, calculate the statistics, and compare with real human accounts.

## 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*. 839–851.

[2] Kayode Sakariyah Adewole, Nor Badrul Anuar, Amirrudin Kamsin, Kasturi Dewi Varathan, and Syed Abdul Razak. 2017. Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications* 79 (2017), 41–67.

[3] R Harald Baayen. 1995. Toni Rietveld and Roeland Van Hout. Statistical Techniques for the Study of Language and Language Behavior. *Functions of Language* 2, 1 (1995), 130–131.

[4] David M Beskow and Kathleen M Carley. 2018. Bot conversations are different: leveraging network metrics for bot detection in twitter. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 825–832.

[5] 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*. 93–102.

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

[7] Chia-Mei Chen, DJ Guan, and Qun-Kai Su. 2014. Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. *Information Sciences* 289 (2014), 133–147.

[8] Aaron Clauset, Cosma Rohilla Shalizi, and Mark EJ Newman. 2009. Power-law distributions in empirical data. *SIAM review* 51, 4 (2009), 661–703.

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

[10] 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*. 273–274.

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

[12] Emilio Ferrara. 2017. Disinformation and social bot operations in the run up to the 2017 French presidential election. *arXiv preprint arXiv:1707.00086* (2017).

[13] Zafar Gilani, Reza Farahbakhsh, Gareth Tyson, Liang Wang, and Jon Crowcroft. 2017. An in-depth characterisation of Bots and Humans on Twitter. *arXiv preprint arXiv:1704.01508* (2017).

[14] 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*. 349–354.

[15] Jennifer Golbeck. 2015. Benford's law applies to online social networks. *PloS one* 10, 8 (2015).

[16] Philip N Howard, Gillian Bolsover, Bence Kollanyi, Samantha Bradshaw, and Lisa-Maria Neudert. 2017. Junk news and bots during the US election: What were Michigan voters sharing over Twitter. *CompProp, OII, Data Memo* (2017).

[17] Philip N Howard and Bence Kollanyi. 2016. Bots,# StrongerIn, and# Brexit: computational propaganda during the UK-EU referendum. *Available at SSRN 2798311* (2016).

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

[19] Leo Katz. 1953. A new status index derived from sociometric analysis. *Psychometrika* 18, 1 (1953), 39–43.

[20] Sneha Kudugunta and Emilio Ferrara. 2018. Deep neural networks for bot detection. *Information Sciences* 467 (2018), 312–322.

[21] Andrea Lancichinetti, Mikko Kivelä, Jari Saramäki, and Santo Fortunato. 2010. Characterizing the community structure of complex networks. *PloS one* 5, 8 (2010).

[22] Kyumin Lee, James Caverlee, and Steve Webb. 2010. Uncovering social spammers: social honeypots+ machine learning. In *Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval*. 435–442.

[23] Sangho Lee and Jong Kim. 2014. Early filtering of ephemeral malicious accounts on Twitter. *Computer Communications* 54 (2014), 48–57.

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

[25] Zachary Miller, Brian Dickinson, William Deitrick, Wei Hu, and Alex Hai Wang. 2014. Twitter spammer detection using data stream clustering. *Information Sciences* 260 (2014), 64–73.

[26] 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*. 467–474.

[27] 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.

[28] 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.

[29] Seth A Myers, Aneesh Sharma, Pankaj Gupta, and Jimmy Lin. 2014. Information network or social network? The structure of the Twitter follow graph. In *Proceedings of the 23rd International Conference on World Wide Web*. 493–498.

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

[31] 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.

[32] 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*.

[33] Bimal Viswanath, M Ahmad Bashir, Mark Crovella, Saikat Guha, Krishna P Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2014. Towards detecting anomalous user behavior in online social networks. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. 223–238.

[34] Jennifer Xu and Hsinchun Chen. 2008. The topology of dark networks. *Commun. ACM* 51, 10 (2008), 58–65.