Analyzing Social Bots and their Coordination during Natural Disasters

Tuja Khaund, Samer Al-Khateeb, Serpil Tokdemir, and Nitin Agarwal

University of Arkansas at Little Rock, Little Rock AR 72204, USA
{txkhaund,sxalkhateeb,sxtokdemir,nxagarwal}ualr.edu

Abstract. Social bots help automate many sociotechnical behaviors such as tweeting/retweeting a message, 'liking' a tweet, following users, and coordinate or even compete with other bots. Social bots exist as advertising bots, entertainment bots, spam bots, and influence bots. In this research, we focus on influence bots, i.e., automated Twitter accounts that attempt to affect or influence behaviors of others. Some of these bots operate independently and autonomously for years without getting noticed or suspended. Furthermore, some of the more advanced influence social bots exhibit highly sophisticated coordination and communication patterns with complex organizational structures. This study aims to explore the role of Twitter social bots during the 2017 natural disasters and evaluate their coordination strategies for disseminating information. We collected data from Twitter during Hurricane Harvey, Hurricane Irma, Hurricane Maria, and Mexico Earthquake that occurred in 2017. This resulted in a total of over 1.2 million tweets generated by nearly 800,000 Twitter accounts. Social bots were detected in the data. Social networks of top bot and top non-bot accounts were compared to examine characteristic differences in their networks. Bot networks were further examined to identify coordination patterns. Hashtag analysis of the tweets shared by bots further helped in identifying hoaxes (such as, 'shark swimming on freeway') and non-relevant narratives (black lives matter, DACA, anti-Semitic narratives, Kim Jong-Un, nuclear test, etc.) that were disseminated by bots in several languages, such as French, Spanish, Arabic, Japanese, Korean, etc., besides English.

Keywords: Social bots, Twitter, natural disasters, crisis events, severe weather, hurricane, earthquake, disinformation, coordination, hoaxes, alternate narratives.

1. Introduction

A bot is a computer application that is designed to perform automated tasks over the Internet. The main idea behind creating a bot is to run simple tasks that are also structurally repetitive, at a rate much higher than humans [1]. A botnet refers to a collection of computer agents or bots that are programmed to act in a coordinated manner. Bots that mimic social behaviors of humans are referred to as social bots. Social bots could be of different types, viz., advertising bots, entertainment bots, spam bots, and influence bots [2]. In this research, we focus on influence bots, i.e., automated or programmed accounts that attempt to affect or influence behaviors of the users with whom they interact. Social bots have various

capabilities, e.g., they can affect users' perceived influence and learn the social graph to analyze people's posts and decide what to say and to whom. With all these capabilities, social bots have inarguably played an active role in affecting public discourse in online spaces (e.g., social media and chat forums) [3]. In this research, we investigate the role of social bots during four natural disaster events, namely *Hurricane Harvey*, *Hurricane Irma*, *Hurricane Maria*, and *Mexico Earthquake* that occurred in 2017. We seek answers to the following questions: (1) Are there characteristic differences between bot networks and human networks?; (2) What are these differences?; (3) Are there hoaxes or alternate narratives being disseminated during these events?; (4) What are these hoaxes and alternate narratives?; and (5) Do bots play a role in disseminating these narratives? To answer these questions, we examine social networks of bots and humans, coordination strategies used by bots, and analyze tweets shared by bots.

2. Literature Review

There is a growing body of research on detecting social bots. Journalists, analysts, and researchers have increasingly reported examples of the potential dangers ushered in by social bots [4]. Widespread diffusion of information by social bots may have unwarranted consequences on society. Social bots reportedly mislead, exploit, and manipulate social media discourse with rumors, spam, malware, misinformation, or simply noise. Sophisticated social bots can generate credible personas, and thus are more difficult for both people and filtering algorithms to detect [4]. In 2010, Z. Chu et al. [5] proposed a classification system to determine whether a tweet belongs to a human, bot, or cyborg [5]. Over 500,000 accounts were studied to find their differences in tweeting behavior and content [5]. Wang et al. [6] have explored the possibility of crowdsourcing bot detection, i.e., using legions of human workers to detect bots. The authors assumed that bot detection is a simple task for humans because humans have a natural ability to evaluate conversational nuances (e.g., sarcasm or persuasive language) and to observe emerging patterns or anomalies. The authors observed the detection rate for hired workers drops off over time, although it remains good enough to be used in a majority voting protocol [6]. Abokhodair et al. [7] studied the "Syrian Social Bots" (SSB) which was used during the Syrian crisis in 2012. The authors focused on one botnet that was active for over eight months before Twitter detected and suspended it. The study analyzed the life and the activities of the botnet where it focuses on the content of the tweets. They found out that bots tend to share more news articles, fewer opinion tweets, no testimonial tweets, and fewer conversational tweets than any other legitimate Arabic or English Twitter user.

3. Methodology

We collected four datasets of Twitter users, using Google TAGS [8], including who tweeted and retweeted about four natural disasters events namely: *Hurricane Harvey, Hurricane Irma, Hurricane Maria*, and *Mexico Earthquake*. The data was collected from 08/30/2017

to 09/28/2017. This resulted in a total of 1,219,454 tweets that were generated by 776,702 Twitter accounts. To analyze persistent bot activity, we filtered down to those twitter accounts that engaged with all the four events. This resulted in 633,903 accounts that either tweeted or retweeted during the four events.

We calculated bot likelihood scores for the accounts using BotOrNot API [9], which ranges between 0 and 100, 100 being the highest likelihood for an account being a bot. For a robust and reliable analysis, we considered top 100 bot accounts (with BotOrNot score ranging between 90% -100%) and top 100 non-bot/human accounts (with BotOrNot score ranging between 0% – 3%). We collected social network (i.e., friends and followers) of the top bot accounts and non-bot/human accounts. Twitter had already suspended some of the bot accounts and some human accounts were set to private, so we were able to collect social network information for 72 bot accounts (Fig 1) and 82 human accounts (Fig 2). We also analyzed the tweets shared by the top bot and non-bot accounts that resulted in 76,928 unique hashtags for the four events.

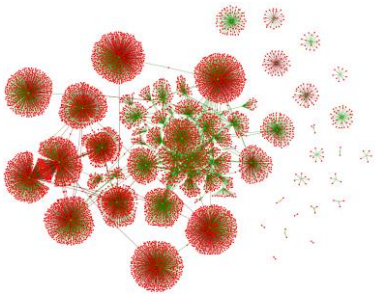


Fig. 1. Bot network, green nodes indicate bots and red nodes indicate their friends and followers.

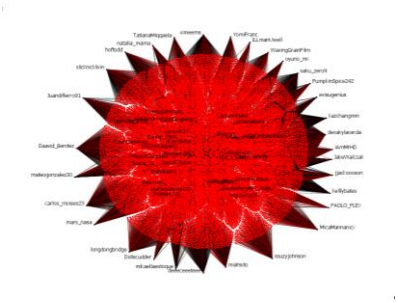
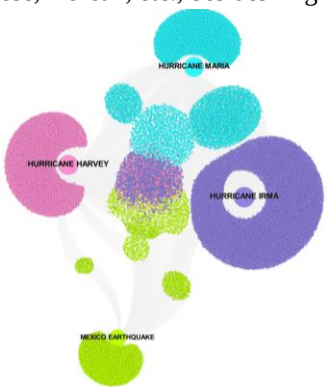


Fig. 2. Human network, black nodes indicate humans, and red nodes indicate their friends and followers.

Community detection algorithm proposed by Vincent et al. [10] which optimize modularity score was run on the bot and human networks. We observed that human networks have more number of communities as compared to bot networks. Furthermore, human communities are smaller in size and denser as compared to bots. In other words, while humans have more tightly knit and focused communities, bots tend to make connections with rather weaker sense of belongingness to a community. Hence, bot communities tend to be bigger and less tightly knit (or less focused connections). Moreover, community detection also revealed strikingly different structural patterns between bots and humans. Bots' communities are more hierarchical in structure, i.e., there is a central core of members who connect more strongly among themselves as opposed to the peripheral members, who are weakly connected with the core as well as among themselves.

In addition to analyzing structural differences between human and bot networks, we examined their content, especially the hashtags. By constructing a hashtag co-occurrence network we identify hashtags that are (1) specific to the event and (2) common across

multiple events. Further applying clustering to the hashtag co-occurrence network [10], we detect four main groups of hashtags (fig 3, left). Colors depict different clusters – one for each disaster event: pink for Hurricane Harvey hashtags, purple for Hurricane Irma, blue for Hurricane Maria, and green for Mexico earthquake. Hashtags common to multiple events were also identified in the hashtag co-occurrence network. Although, majority of the common hashtags refer to support, relief operations, prayers, and solidarity for the victims during these disaster events, we did observe a substantial presence of non-related hashtags that were common to multiple events. More troubling was the strategy bots used in pushing these non-related hashtags, i.e., non-related hashtags were latched on to the event-related hashtags. These non-related hashtags included hoaxes (such as 'shark swimming on freeway') and alternate narratives ('black lives matter', deferred action for childhood arrivals - commonly known as DACA, anti-Semitic narratives, Kim Jong-Un, nuclear test, etc.) that were disseminated by bots in several languages, such as French, Spanish, Arabic, Japanese, Korean, etc., besides English (fig. 3, right).



Language	Hashtag (Translation)
English	#DACA, #BlackLivesMatter
Spanish	#VenezuelaDemocraciaYDiálogo (Venezuela Democracy and Dialogue), #Cáncer (Cancer)
Arabic	(The demise Of Israel) #زوال_إسرائيل, (The Jews) #اليهود
French	#Nucléaire (Nuclear), #GendarmerieEnOpération (Gendarmerie Special Operations)
Japanese	金正恩 (Kim Jong-un), 核试验 (Nuclear Test)

Fig. 3. Hashtag co-occurrence network (left) for the four natural disaster events in 2017 and non-relevant hashtags and their stated language (right).

On digging deeper, we found 765 tweets that discussed the *Shark* hoax. We ran a modularity community detection algorithm on the tweet-retweet network which resulted in 69 clusters as shown in figure 4 (left) - colors depict different clusters - with the biggest cluster in blue. The blue cluster refer to a tweet "*A shark photographed on I-75 just outside of Naples, FL This is insane. #HurricaneIrma*" that was retweeted 420 times. We found that few accounts that disseminated the tweet had greater than 80% bot scores while a majority of the accounts had less than or equal to 50% bot scores (see, figure 4, right). Although the majority of the accounts had 50% or lower bot scores many of these accounts exhibit bot-like behaviors. One possible explanation is that these accounts may have helped dissemination of the hoax without proper fact-checking. Alternatively, these accounts could be sophisticated bots that mimic human behavior to remain undetected by Twitter bot detection algorithms. Further research is needed to clarify the nature of these accounts.

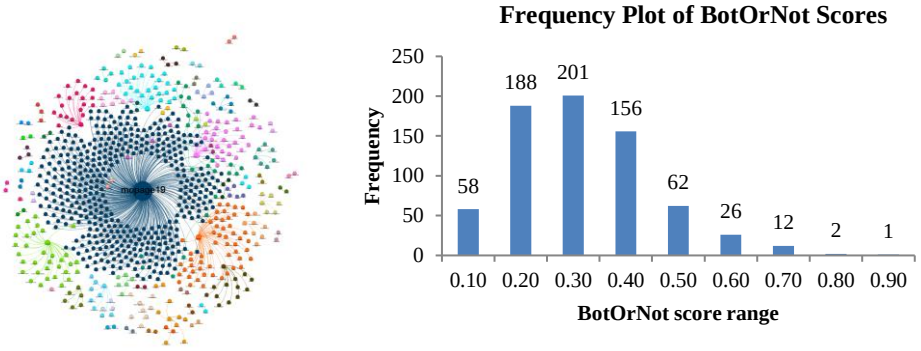


Fig. 4. Retweet network (left) of users who shared the 'shark' hoax during the four natural disaster events in 2017 and their bot scores (right).

4. Conclusion and Future Work

Social bots can disrupt discourse in online spaces. Social bots evolve constantly and become more sophisticated over time. We compared the social networks of bot and non-bot accounts that were identified during the 2017 natural disaster events. We observed, while humans have more tightly knit and focused communities, bots tend to make connections with rather weaker sense of belongingness to a community. Analysis of their content revealed that the discourse was not just limited to the disaster events. Non-relevant hashtags including hoaxes and alternate narratives were latched on to the event-specific hashtags and were disseminated in Spanish, Arabic, French, Japanese, among other languages.

The overarching research agenda is to investigate the different strategies that social bots use to coordinate disinformation campaigns and successfully manipulate online discourse. For future work, we will investigate the accounts that exhibit bot-like behavior despite having a low bot score. We will compare the communication network of bot and human accounts to identify other information maneuver tactics. We plan to expand our analysis to include entertainment and sport events to study the role of social bots in disseminating hoaxes, alternate narratives, uncertain, or ambiguous information.

Acknowledgments

This research is funded in part by the U.S. National Science Foundation (IIS-1636933, ACI-1429160, and IIS-1110868), U.S. Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489, N00014-15-P-1187, N00014-16-1-2016, N00014-16-1-2412, N00014-17-1-2605, N00014-17-1-2675), U.S. Air Force Research Lab, U.S. Army Research Office (W911NF-16-1-0189), U.S. Defense Advanced Research Projects Agency (W31P4Q-17-

C-0059) and the Jerry L. Maulden/Entergy Fund at the University of Arkansas at Little Rock. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations. The researchers gratefully acknowledge the support.

References

1. Gayer, O.: What is an Internet Bot | How Bots Can Hurt Your Business, https://www.incapsula.com/blog/understanding-bots-and-your-business.html.
2. Types of Bots: An Overview of Chatbot Diversity | botnerds.com, http://botnerds.com/types-of-bots/.
3. @DFRLab: Le Pen's (Small) Online Army, https://medium.com/dfrlab/le-pens-small-online-army-c754058630f0, (2017).
4. Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A.: The rise of social bots. Commun. ACM. 59, 96–104 (2016).
5. Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S.: Who is tweeting on Twitter: human, bot, or cyborg? In: Proceedings of the 26th annual computer security applications conference. pp. 21–30. ACM (2010).
6. Wang, G., Mohanlal, M., Wilson, C., Wang, X., Metzger, M., Zheng, H., Zhao, B.Y.: Social turing tests: Crowdsourcing sybil detection. ArXiv Prepr. ArXiv12053856. (2012).
7. Abokhodair, N., Yoo, D., McDonald, D.W.: Dissecting a social botnet: Growth, content and influence in Twitter. In: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. pp. 839–851. ACM (2015).
8. Hawksey, M.: TAGS v6.0ns, https://docs.google.com/spreadsheets/d/1EqFm184RiXsAA0TQkOyWQDsr4eZ0XRuSFryIDun_AA4/edit?pli=1&usp=embed_facebook&usp=embed_facebook.
9. Botometer by OSoMe, https://botometer.iuni.iu.edu.
10. Blondel, V.D., Guillaume, J.-L., Lambiotte, R., Lefebvre, E.: Fast unfolding of communities in large networks. J. Stat. Mech. Theory Exp. 2008, P10008 (2008).