Investigating the Use of Bots to Spread Fake News in Social Media

Sumeet Kumar

Carnegie Mellon University
5000 Forbes Ave, Pittsburgh, PA 15213, USA
Email: sumeetku@cs.cmu.edu

1 Introduction

Fake news is not new. However, the phenomenal growth of online social media coupled with ease in publishing unverified content and click based advertisement revenue, have increased the use of fake news to drive discussions. Though often considered innocuous, it can have high social cost. For example, Allcott and Gentzkow [1] in their study on 2016 presidential election, find around 38 million shares of fake news on Facebook, with 30 million pro-Trump and 7.6 million pro-Clinton shares. Parkinson [7] reported that the inactivity of social-media companies in removing fake-news might have contributed to the results of the 2016 US presidential election. Either for spreading ideologies or for making money, the goal of fake news creators is to spread their message rapidly, so the likely use of bots (or human assisted bots) in the process is hard to dismiss. However, most existing research on fake-news have considered the origin [8], the motivations [1] and the impact of fake news [7], but not the use of bots. In our investigation, we have found social bots [6] that are actively being used on Twitter to fool the content promotion algorithms and spread specific agenda. In this research, we use network analysis to understand how social botnets are used for the faster dissemination of fake news, and try to find the motivations behind such sharing by jointly analyzing the bots behavior and the change of network structure over time. Besides, we also investigate the syntactic characteristic of social-media posts related to fake-news on Twitter, including the use of hashtags, user-mentions and sentiment that make fake news more appealing to particular groups.

2 Problem Statement

Most existing work on detecting fake news have taken a machine learning approach to classify news as fake or otherwise. This classification approach does not point to the motivations behind spreading such news. We take a network analysis based approach to understand the motivations behind spreading of fake news. We expect two prime motivations [1], a) pecuniary i.e. be a part of the ‘digital gold rush’ b) ideological i.e. to seek to advance the stand the spreaders have. In our investigation on Ukrainian Tweets, We have found bots promoting fake news. Given the active monitoring of anti-social activities by social-media companies, it's hard to build and maintain and an army of bots. We expect that the content creators who spread fake-news for money, use their bots for multiple purposes. In contrast, those who use fake-news for ideological reasons, stick to one objective but target many vulnerable groups of users. Thus, a better understanding of the bot usage could support improved reasoning about the motivations behind spreading fake news.

3 Dataset, Proposed Method and Current Progress

We generate our dataset by collecting Tweets relevant to the Euromaidan movement. The Euromaidan movement started as a series of protests in November 2013, where large numbers began to call for the removal of then Ukrainian President Viktor Yanukovych. These protests reached their peak in February 2015, ultimately leading to the removal of many of Ynukovych's senior 98 officials, and were a precursor to Russia's subsequent occupation of Crimea. We download tweets data based on search terms, geo-coordinates based filtered search, and snowball sampling approach. We then filter the tweets that have embedded URLs. Using a known set of fake URLs obtained from experts on Ukranian issues, we divide the entire dataset into fake and non-fake tweets. We then build networks of users, user-tweets, user-mentions and user-hashtags. The visualizations of these networks (Fig. 1) give us an idea on how the network structure around fake-news differs from the non-fake news networks, and how these structures changed over time. We also analyzed the content of each of web-pages linked to these URLs.

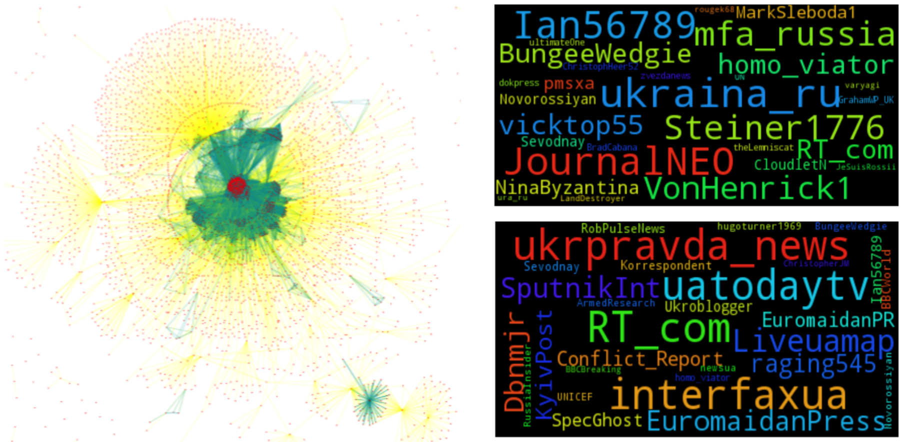

Figure 1. Left image shows different Twitter-users (red dots) spreading fake-news and their network in our Ukrainian Tweets dataset. The yellow lines are mention links and the green lines are co-hashtag links. The top plot on right shows the top mentions used in tweets that have embedded URLs related to fake news. The bottom plot on right shows the top mentions used in tweets with non-fake embedded URLs.

In our previous work [2,3,4,5], we have used social-media posts and news to better understand social issues and security risks. In a more recent work, we used deep learning approach to understand emotions in multimedia posts. The usage of multi-media in social media posts have increased a lot, but sentiment analysis tools primarily used language. To improve the current state of sentiment analysis, which is text heavy, we developed a deep-learning model to predict emotions in images. Emotions in images could be combined with the sentiment in the text to better gauge the feeling evoked in multi-media posts. We are working on combining sentiment analysis, changes in network structure over time and bots behaviors to learn the motivations behind sharing the fake news.

4 Future Directions and Advices Sought

Our investigation has revealed the use of bots to promote tweets. We have observed a clear distinction in approaches of spreading fake-news and general news. In particular, the use of a higher number of mentions to get tractions (Fig.1) and more use of different hashtags tailored to attract a particular community. Our investigation also shows a greater level of emotional variability in the content of fake news. We seek advice on ways to better understand the bots behavior on Twitter. In particular, their reuse and finding ways to identify them. We hope to merge the knowledge gained by analyzing bots behavior and the dynamic network structure of the community where they operate, to better understand the motives behind sharing fake-news.

References

1. Allcott, H., Gentzkow, M.: Social media and fake news in the 2016 election. Journal of Economic Perspectives 31(2) 211-36. (2017)
2. Kumar, S., Benigni, M., Carley, K.M.: The Impact of US Cyber Policies on Cyber-Attacks Trend. In: Intelligence and Security Informatics (ISI), 2016 IEEE International Conference on. Tucson, Arizona USA (Sep 2016)
3. Kumar, S., Carley, K.: Understanding DDoS Cyber-Attacks using Social Media Analytics. In: Intelligence and Security Informatics (ISI), 2016 IEEE International Conference on. Tucson, Arizona USA (Sep 2016)
4. Kumar, S., Carley, K.M.: Approaches to Understanding the Motivations Behind Cyber Attacks. In: Intelligence and Security Informatics (ISI), 2016 IEEE International Conference on. Tucson, Arizona USA (Sep 2016)
5. Kumar, S., Carley, K.M.: DDoS Cyber-Attacks Network: Who's Attacking Whom. In: Intelligence and Security Informatics (ISI), 2016 IEEE International Conference on. Tucson, Arizona USA (Sep 2016)
6. Morstatter, F., Wu, L., Nazer, T.H., Carley, K.M., Liu, H.: A new approach to bot detection: striking the balance between precision and recall. In: Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on. pp. 533–540. IEEE (2016)
7. Parkinson, H.J.: Click and elect: how fake news helped donald trump win a real election. The Guardian (2016)
8. Samanth, S.: Inside the macedonian fake-news complex. Wired.com (2017), https://www.wired.com/2017/02/veles-macedonia-fake-news/