# Stweeler: A Framework for Twitter Bot Analysis

Zafar Gilani, Liang Wang, Jon Crowcroft
University of Cambridge
{szuhg2, lw525, jac22}
@cam.ac.uk

Mario Almeida
Polytechnic University of Catalonia
mario.almeida
@est.fib.upc.edu

Reza Farahbakhsh
Institut Mines Telecom
CNRS Lab UMR5157
reza.farahbakhsh
@it-sudparis.eu

## ABSTRACT

The WWW has seen a massive growth in variety and usage of OSNs. The rising population of users on Twitter and its open nature has made it an ideal platform for various kinds of opportunistic pursuits, such as news and emergency communication, business promotion, political campaigning, spamming and spreading malicious content. Most of these opportunistic pursuits are exploited through automated programs, known as bots. In this study we propose a framework (***Stweeler***) to study bot impact and influence on Twitter from systems and social media perspectives.

## Keywords

information dissemination; bot analyser; content analysis

## 1. INTRODUCTION

Twitter has seen a massive rise in bot population. This is owed to a number of reasons: due to soft inspection during registration (an email address, a CAPTCHA recognition and a phone number are the only requirements), but mostly due to the Twitter API that lets programmers automate actions on Twitter. Studying the bot phenomena in social media is important on two accounts. Firstly, by understanding system dynamics, determined by user behaviour (human or bot), we can build adaptive systems. Secondly, we can study the impact of human-bot interaction from sociological perspective. To the best of authors' knowledge previous studies did not pay ample attention to this nascent field of research, and previous efforts focus mainly on detecting spam in Twitter [5] or identifying bots based on the context of tweets [1]. A multitude of things are not even known about bots. In this study we propose a framework to analyse bot behaviour in Twitter. We focus on bots in Twitter primarily because of two reasons: (1) Twitter content is mostly public and (2) studies [1] indicate a substantial presence of automated programs on Twitter.

## 2. RESEARCH QUESTIONS

This section includes a set of interesting research questions for bot analysis and devise a framework (see Section 3) to answer them.


*WWW'16 Companion,* April 11–15, 2016, Montréal, Québec, Canada.
ACM 978-1-4503-4144-8/16/04.
http://dx.doi.org/10.1145/2872518.2889360 .

**About bots**: The first key aspect is about the nature of bots. Why do bots exist in digital world and why do we see such quantity of bots in a large OSN such as Twitter. To answer these questions we need to understand the behaviour of bots in terms of their activities, e.g. ratio of tweets, type of tweets, tweet originality (retweets vs. new tweets), and tweet properties (URLs, text).

**Bot usage and impact**: The second interesting aspect is the usage and impact of bots on OSNs. How do different entities, e.g. news corps or commercial enterprises, use bots to disseminate content? There are a set of bots that do not impact OSNs such as those that passively collect data (from Twitter's Streaming or Firehose APIs). Bots that have impact on OSNs are those that disseminate information or content such as news corps, commercial enterprises, spammers and other content generators. Furthermore, do bots influence content popularity, such as making topics 'trend' or preventing others from being 'trending'? For Twitter, bots can be a mixed bag - beneficial in terms of popularity, visibility and financial aspect vs. detrimental in similar aspects? Can bots impact the network, such as affect content placement or caching strategies in CDNs?

**Bot weight**: We can consider weight as the content that bots produce as well as the engagement that they attract. Do bots generate original content (some examples include earthquakeBot, parliamentedits, congressedits, ecurrie1970, a_quilt_bot)? What percentage of produced content are from bots? Can we predict and cache this bot generated content? How do bots interact with Twitter's own promotion algorithm? Do bots make Twitter more active due to the number of followers they have? Do they form majority of Twittersphere by forming multiple largest connected components of the Twitter graph?

**Bots vs. humans**: How much activity and content is generated by bots and how much is generated by humans? Who is major content producer and who is a major content consumer? What is the degree of similarity between content produced by humans and content produced by bots? Which attracts more attention or which drives popularity and why?

## 3. METHODOLOGY AND FRAMEWORK

This section describes our framework, namely ***Stweeler***[1], and its two main parts: bot and analyser. Fig. 1 illustrates how our Twitter bot works. (1) The bot fetches a trending topic or a popular tweet, disassembles the information in the topic or tweet, such as text and URL. (2) The URL is then fetched into our web server (WS), which has a shortener module running inside. The shortener shortens the URL into tnyurl.uk domain name. The shortener is also responsible for maintaining a database for shortened URLs. (3) The bot then reassembles the tweet using the text and shortened URL. (4) The

[1]***Stweeler***- `https://github.com/zafargilani/stcs`

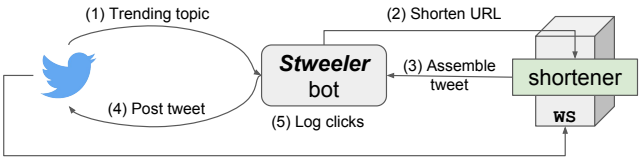


**Figure 1: How *Stweeler* bot works.**

tweet is finally posted to the Twitter system using `tweet(text)` function of the Twitter API. (5) Whenever, a Twitter user clicks on our URL, our WS records the click and a collection of useful data for later analysis. This information is listed in Table 1. Please note that in order to respect the ethical boundaries of social media research, we **only** collect publicly available data about users and hash sensitive information such as IP addresses.

**Table 1: Data collected via click logging.**

| Data attribute | Description |
|---|---|
| Click timestamp | Date and time of click, local to our web server. |
| Tweet ID | Tweet ID which produced a click. |
| Hashed IP address | Hashed IP address of the machine that clicked the URL in the tweet identified by Tweet ID. This is recorded to witness revisits of the same Twitter user for the same URL. |
| User agent string | This records the `HTTP_USER_AGENT` string of the Twitter user clicking the URL in the tweet identified by Tweet ID. |

The ***Stweeler*** analysis framework in Fig. 2. has inputs (left), toolkit (centre) and outputs (right). The bot analyser takes user data and tweet content as input to process it through its internal components. Bot behaviour has been found to be often less complex than that of humans [2, 3]. This can be measured using entropy rate, where low entropy indicates regular nature and high entropy indicates random nature of a process. To estimate this entropy, the bot can utilise corrected conditional entropy as defined in [4] and as exploited in [1]. Additionally, some of the Twitter account properties can also be very helpful for user classification. Properties as indicated and measured in [1] include URL ratio per tweet (much higher for bots), tweeting device makeup (bots use API and humans use Web or mobile), following to followers ratio (much higher for bots than humans) and link safety (whether a link is malicious or not). These could be used as a supplementary to decide between bots and humans. Similarly, an NLP or Bayesian text classification can be used to detect spam in tweets and classify usage of bots.

The content analyser dissects content based data such as trends, topics, keyword, popular hashtags and geolocation to provide bot impact on Twitter in terms of activity and data volume generated, bot influence on Twitter in terms of followers, and how much the bots morph OSNs and relationship trees. The ever-growing bot population will have a potential impact on CDNs and caching systems in future. The nature of the bot (content producer or consumer) will determine the nature of the impact. Moreover, the content analyser uses Bayesian text classification as well as ranking algorithms to rank credibility of information. This could lead to credibly categorising data into advertisements (for e-commerce such as LBA and LBS), trending or news, and informative content.

## 4. INITIAL ANALYSIS

This section includes an initial analysis from a trial run of the framework for a period of one month from 2015-11-21 to 2015-12-18. In this period we have collected a dataset of click logging (Step 5 in Fig. 1) and surprisingly we found that out of 12,000 clicks for

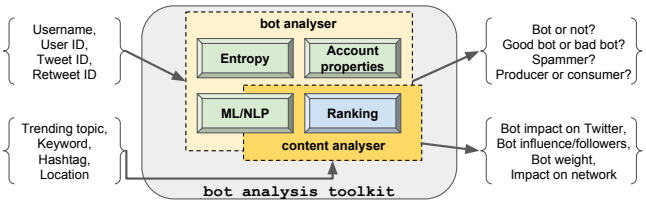


**Figure 2: *Stweeler* analysis framework.**

the URLs we shorten and post, about 4,500 are from entities that advertise themselves as bots[2]. This constitutes 37.5% of activity (over $\frac{1}{3}$) that is emanating from automated programs. Moreover, we also measure revisits for a URL from the same entity. In our dataset so far we find over 1,000 instances of bots making revisits to our URLs within a few seconds. This is probably due to a bot's requirement to find content and either perform a direct retweet or copy a tweet into a visually new one.

We also looked at the most popular bots on Twitter to find properties such as their nature (original content producer, disseminator, etc.), likes-to-tweets ratio, and followers-to-following ratio. We found that out of the 30 random popular self-advertised bots, 21 of those produce original content in terms of text or image, while 11 of them produce useful content (emergency communication, news, notifications and answering questions). Out of 30 of these bots, only one bot had a likes-to-tweets ratio of 1 or more, only one other had above 0.2, and much to our surprise most had it below 0.1. As for followers-to-following ratio, only two bots have a ratio close to 1, implying strong reciprocity which is typical of human relationships [1]. Rest of the bots have much larger number of followers than following (the ratio is typically 1,000 to 1).

## 5. CONCLUSION AND FUTURE WORK

Bots widely exist in OSNs. They contribute a significant amount of activities, both consume and produce content, and even interact with human users. As the analysis on human behaviours is crucial to understanding OSNs, a thorough research on bot demography is equally important. Therefore, in this poster, we presented a list of important questions, and further implemented a framework namely ***Stweeler*** as an effective tool to study the bot community. As our future work, we aim to answer the raised questions by using the ***Stweeler*** analysis framework to have comprehensive understanding of the bot population.

**Acknowledgement:** This work is funded by EU Metrics project (Grant EC607728), Celtic Plus CONVINcE and ITEA CAP.

## 6. REFERENCES

[1] Chu, Z., Gianvecchio, S., Wang, H., and Jajodia, S. Who is tweeting on twitter: Human, bot, or cyborg? In *ACSAC '10*, ACM.

[2] Gianvecchio, S., and Wang, H. Detecting covert timing channels: An entropy-based approach. In *CCS '07*, ACM.

[3] Husna, H., Phithakkitnukoon, S., and Dantu, R. Traffic shaping of spam botnets. In *CCNC 2008*, IEEE.

[4] Porta, A., Baselli, G., Liberati, D., Montano, N., Cogliati, C., Gnecchi-Ruscone, T., Malliani, A., and Cerutti, S. Measuring regularity by means of a corrected conditional entropy in sympathetic outflow. *Biological Cybernetics 78*, 1 (1998).

[5] Wang, A. H. Don't follow me: Spam detection in twitter. In *SECRYPT 2010*.

[2]We search for keyword 'bot' in the `HTTP_USER_AGENT` string or associated webpage that says it is a bot.