

Figure 1: How *Steeeler* 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 <code>HTTP_USER_AGENT</code> string of the Twitter user clicking the URL in the tweet identified by Tweet ID.

The *Steeeler* 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

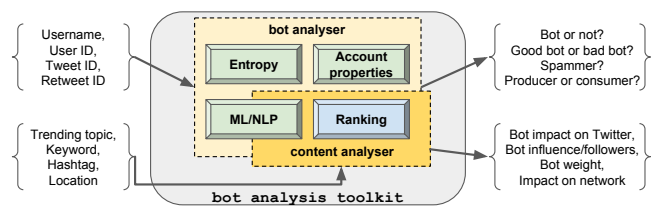


Figure 2: *Steeeler* analysis framework.

the URLs we shorten and post, about 4,500 are from entities that advertise themselves as bots². 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 *Steeeler* as an effective tool to study the bot community. As our future work, we aim to answer the raised questions by using the *Steeeler* analysis framework to have comprehensive understanding of the bot population.

Acknowledgement: This work is funded by EU Metrics project (Grant EC607728), Celtic Plus CONVINC 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., PHITHAKKITNUKON, 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 *SECURITY 2010*.

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