Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet

Authors: Simon Hegelich and Dietmar Janetzko
Presented by: Samer Al-khateeb

Accepted as a Poster and presented at the 10th International Conference on Web and Social Media (ICWSM), Cologne, Germany, May 17-20

Department of Information Science
Center of Social Media & Online behavioral Studies (COSMOS)
University of Arkansas at Little Rock (UA Little Rock)

Overview/Big Picture

- They analyzed a social botnet contents involved in the Ukrainian/Russian conflict.
- They used text mining and unsupervised machine learning, here *clustering*.
- They identify three different botnet behaviors:
  - **Mimicry:** The bots try to hide their bot-identity.
  - **Window Dressing**: To be interesting to normal users they are promoting topics by pushing hashtags and
  - **Reverberation:** retweeting selected Tweets and messages.

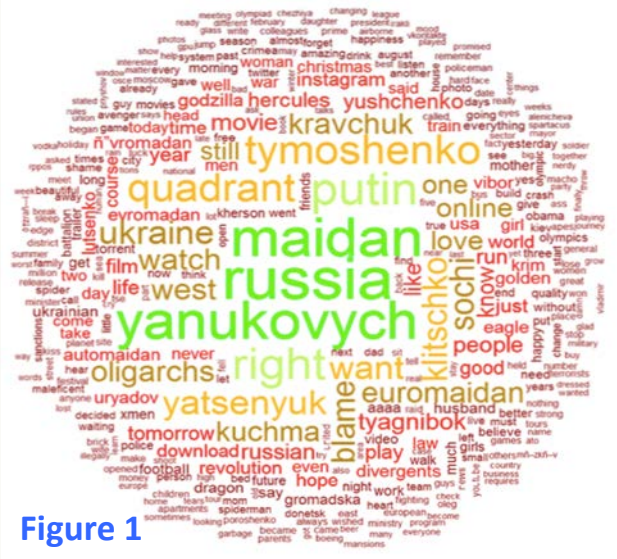
Experiment Details:

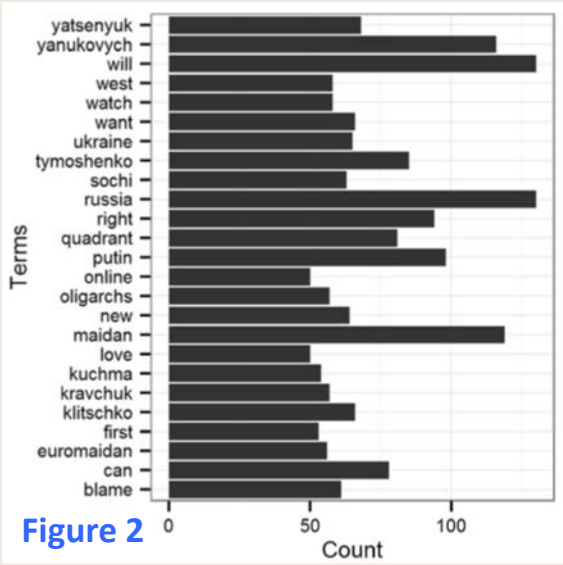
- **Dataset Info:**
  - They collected Tweets that contain **the hashtag "#Ukraine"**, for 24 hours via the Twitter streaming API on **February 22th, 2014** (which is the day of the impeachment of former Ukraine President Janukovitsch).
  - They obtained data with identical texts not labelled as "retweet" in the meta-data, (which is unlikely for normal users).
  - They identified **86 of the Twitter accounts** as social bots: because Twitter-meta-data contains information about the status source, i.e., the URL from which the Tweet was sent. Following this URL, we could identify **twifarm** a program designed to manage huge numbers of social bots on Twitter.
  - They traced **friends and followers** of the social bots, checked their status sources, too. Removal of duplicates led to a sample of **1740 social bots**.
  - They **translated each of the tweets** via the Google translation API from Ukrainian and Russian to English and **pre-processed all Tweets** (removing punctuations, transferring to lower characters, removing stop- words).

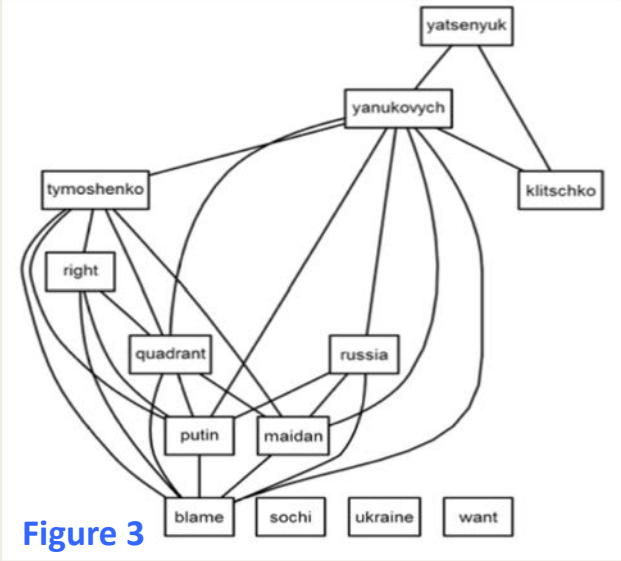
Experiment Details Continue…..

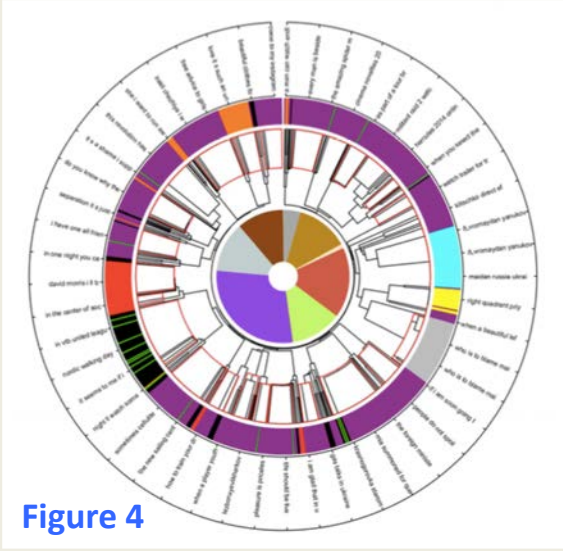
- **Text Mining & Machine Learning Algorithms used:**
  1. **Descriptive Text mining**:
     - They generated a **word cloud** to see the most occurred words (Fig. 1).
     - Analyzed the **most frequent words** (Fig. 2).
     - Calculation of **word-word correlations** and visualization as a network, which revealed connections between terms across the Tweets (Fig. 3).
  2. Conducting different methods of **cluster-analysis**:
     - **Partitional Clustering** --> K-means --> Hartigan-Wong-algorithm (data element has to be only in one cluster (no overlapping))
     - **Hierarchical Clustering** --> (data element can be in more than one cluster) Hierarchical cluster-analysis (Fig. 4).

Research Findings









Research Findings Continue …..

- They run the algorithm with (k= 2-15) each time they calculated **the sum of squared error (SSE)** for different numbers of clusters **8 emerged as a good number of clusters** as the SSE decreases only lightly with an additional cluster.
- **The k-means cluster** analysis clearly distinguished between political (“signal”) and non-political Tweets (“noise”) in the social botnet. This is remarkable as the biggest cluster is characterized by non-political content.
- Both clustering approaches lead to comparable results.
  - The results are mainly robust in the bootstraping procedure.
  - **The k-means approach** finds one big class of “noise” and several classes of political “signals” while
  - **the hierarchical** clustering differentiates the “signal” in useful subgroups.

Research Findings Continue …..

- The social botnet studied exhibits three distinctive *patterns of behavior*:
  - **Mimicry**: The bots try to hide their bot-identity.
  - **Window Dressing**: To be interesting to normal users they are promoting topics by pushing hashtags
  - **Reverberation:** retweeting selected Tweets and messages.
  - The bots try to ***hide their bot identity***; by being ***interesting to normal users*** whilst promoting topics via pushing hashtags and ***retweeting selected Tweets***.
- The study *revealed that*:
  - The behavior of the bots is not guided by a simple deterministic structure of command and obedience between a human bot master and an army of bots. **Instead**, the politically relevant behavior results from complex algorithms leading to a high degree of autonomy of the bots:
  - The bots are not doing something they have been directly told. **Instead,** they follow abstract rules like “Take a popular tweet and add the following hashtags”.
  - In addition, most of the time, the bots are not following their direct “mission”. **Instead**, they use algorithms mirroring the behavior of normal users.
  - This makes it extremely hard to identify the bots and to understand their political aim.

Thank you

Questions?