Leveraging network topology for better fake account detection in social networks*

Proposal presentation

Björn Bebensee
bebensee@snu.ac.kr

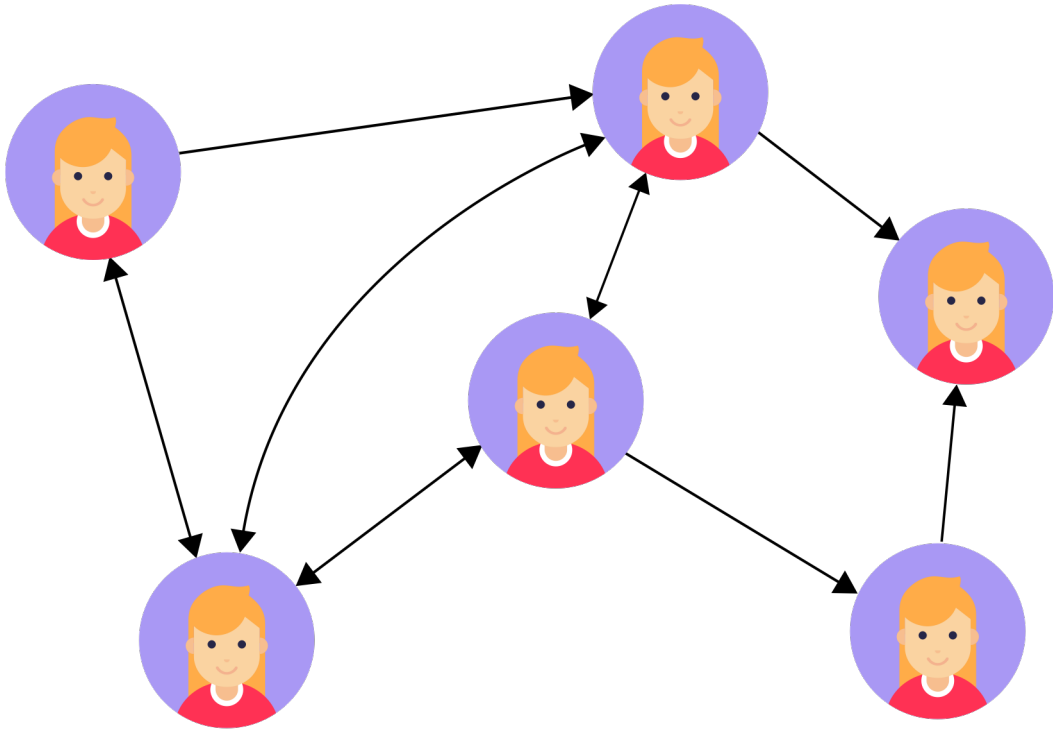
Nagmat Nazarov
nagmat@snu.ac.kr

*working title

Motivation

High number of fake accounts in social networks

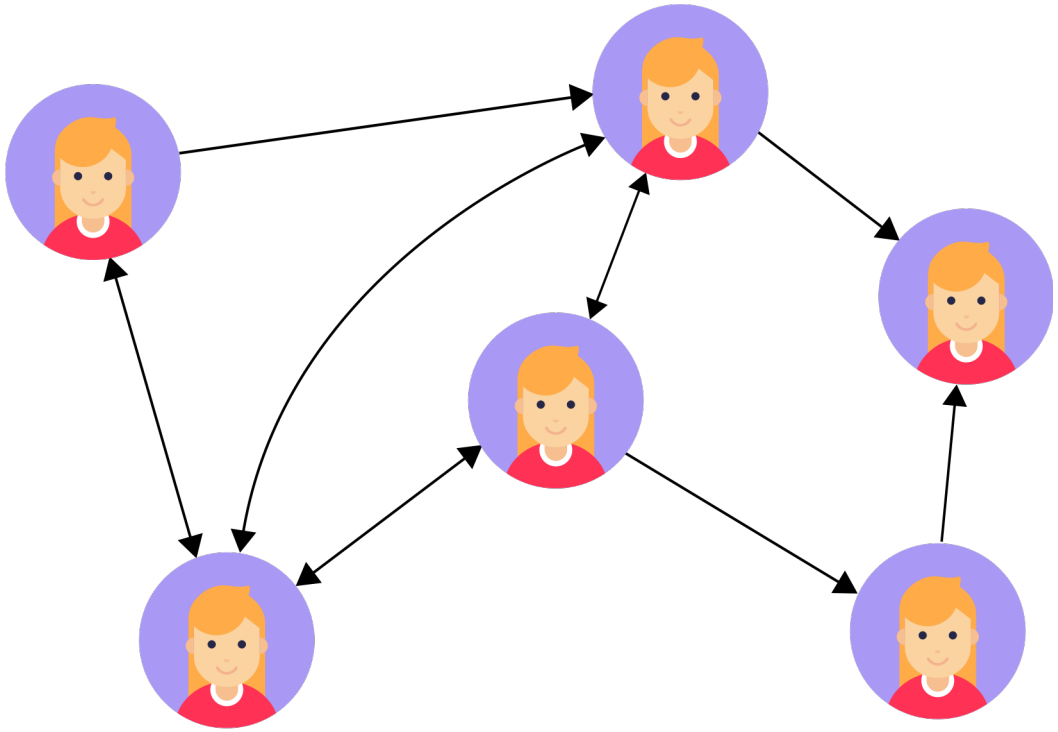
Fake accounts typically serve malicious purposes!



Problem definition

Given: directed graph G=(V,E) of users and their interactions

Goal: identify all users that are fake accounts



Dataset

Use labelled data by Cresci, 2018.

Total: 25987 accounts, 7479 human, 18508 bots.

However: Twitter does not allow sharing of user data online. Dataset only contains (user_id, label) pairs.

Dataset

Scraped user data from Twitter ourselves.

But: many of the users from original dataset have been deleted (mostly bots).

Scraping challenging due to very low API request limits.

Dataset

Scraped data:

13,091 user profiles (~49.6% of accounts less than original dataset, rest has been deleted or is a locked account).

6,082 human accounts.

7,009 bot accounts.

Dataset became more balanced!

Dataset

Retrieved data for each user:

- user_id
- label
- username
- screen_name
- number of “followers” (in-degree)
- number of “following” (out-degree)
- location (if set)
- url (if set)
- description (if set)
- listed_count
- favourites_count
- status_count
- created_at
- default_profile
- default_profile_image
- following_list (up to 5000)
- follower_list (up to 5000)

Dataset

Additionally: retrieved all this profile data for each account in following_list and follower_list.

Data for total of 4.6M accounts, ~13,000 labelled accounts.

Problems

90^{th} percentile effective diameter of Twitter: 4.8 (Kwak et al., 2010)

Number of triangles or finding (strongly) connected subgraphs is infeasible for us, requires crawling with depth=3.

Social graph

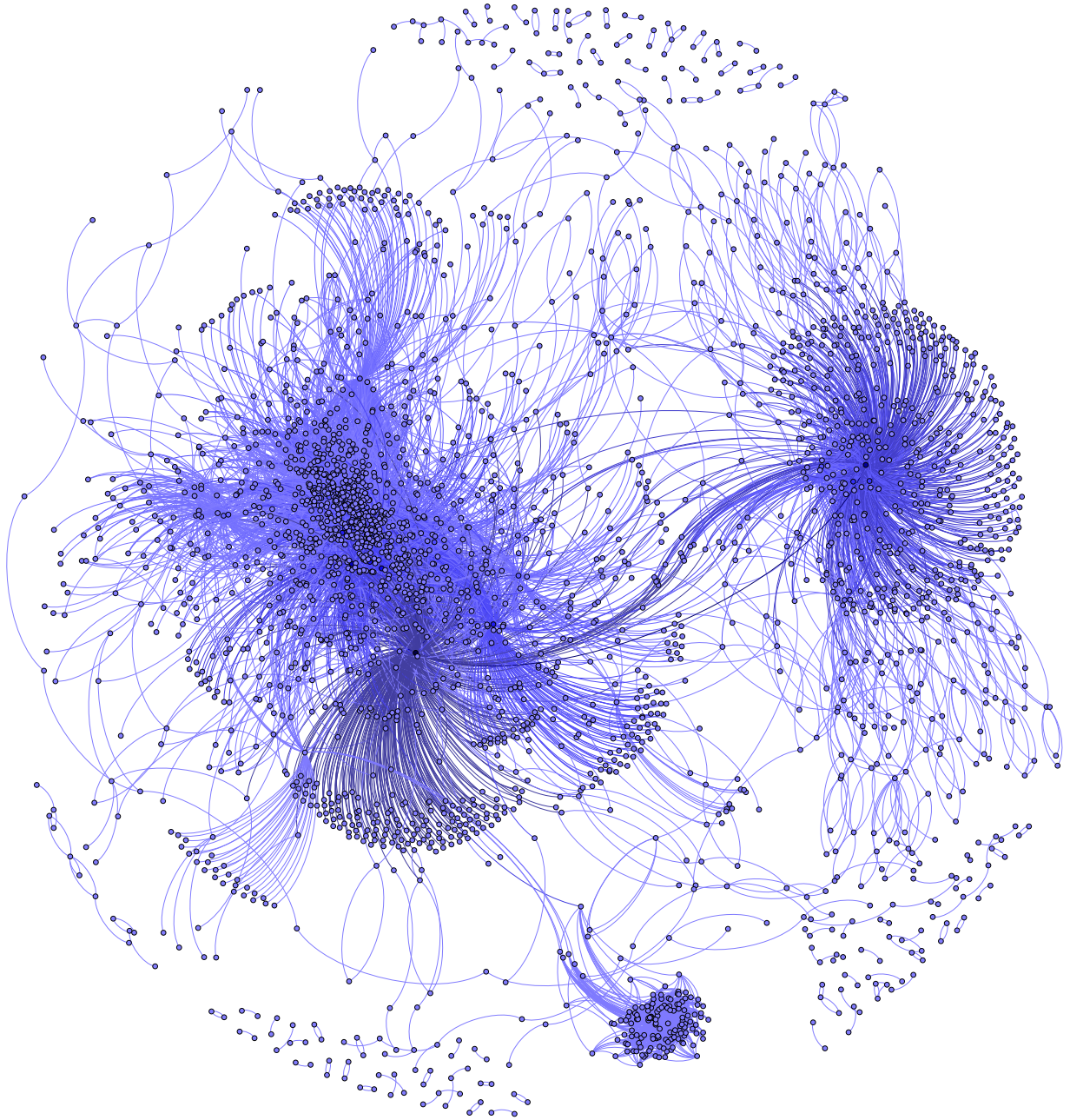
We created the social graph using collected data. Some statistics:

Vertices: 4,611,170

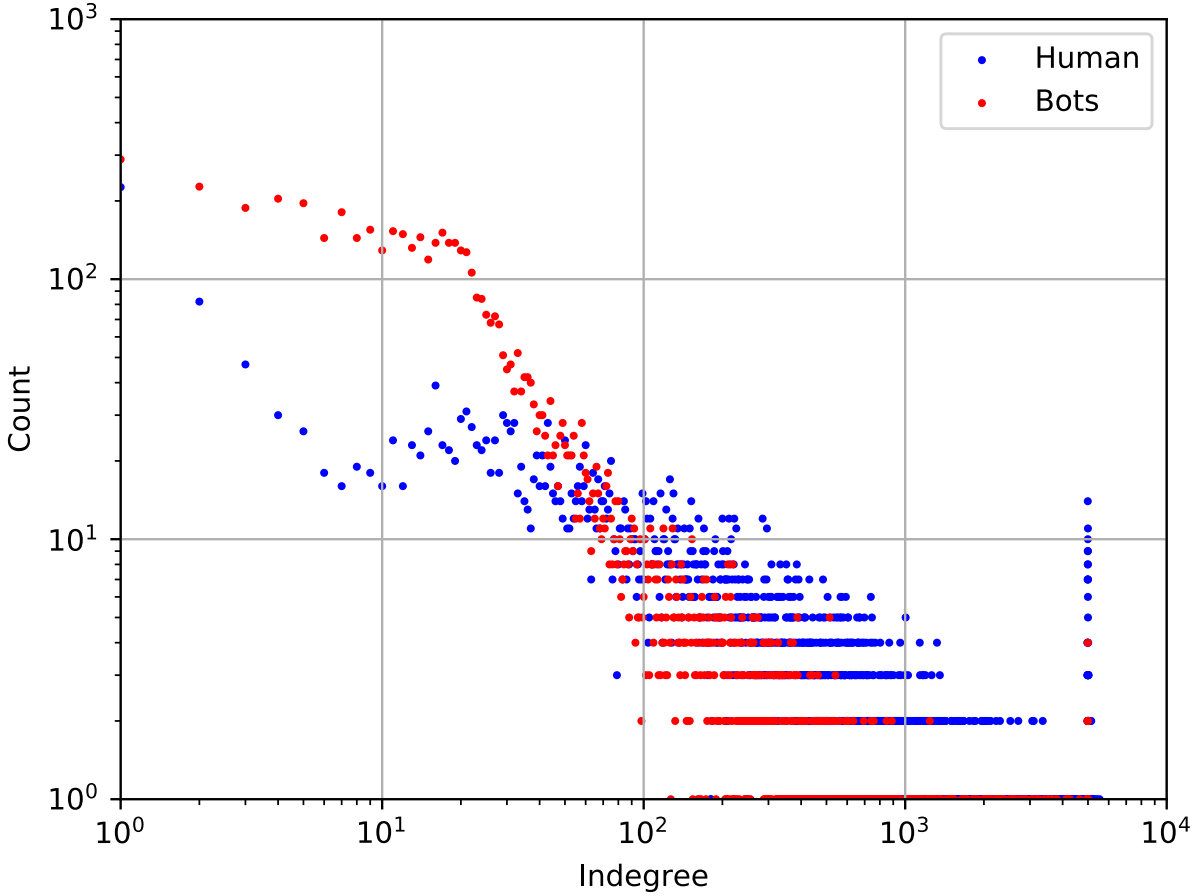
Edges: 8,514,389

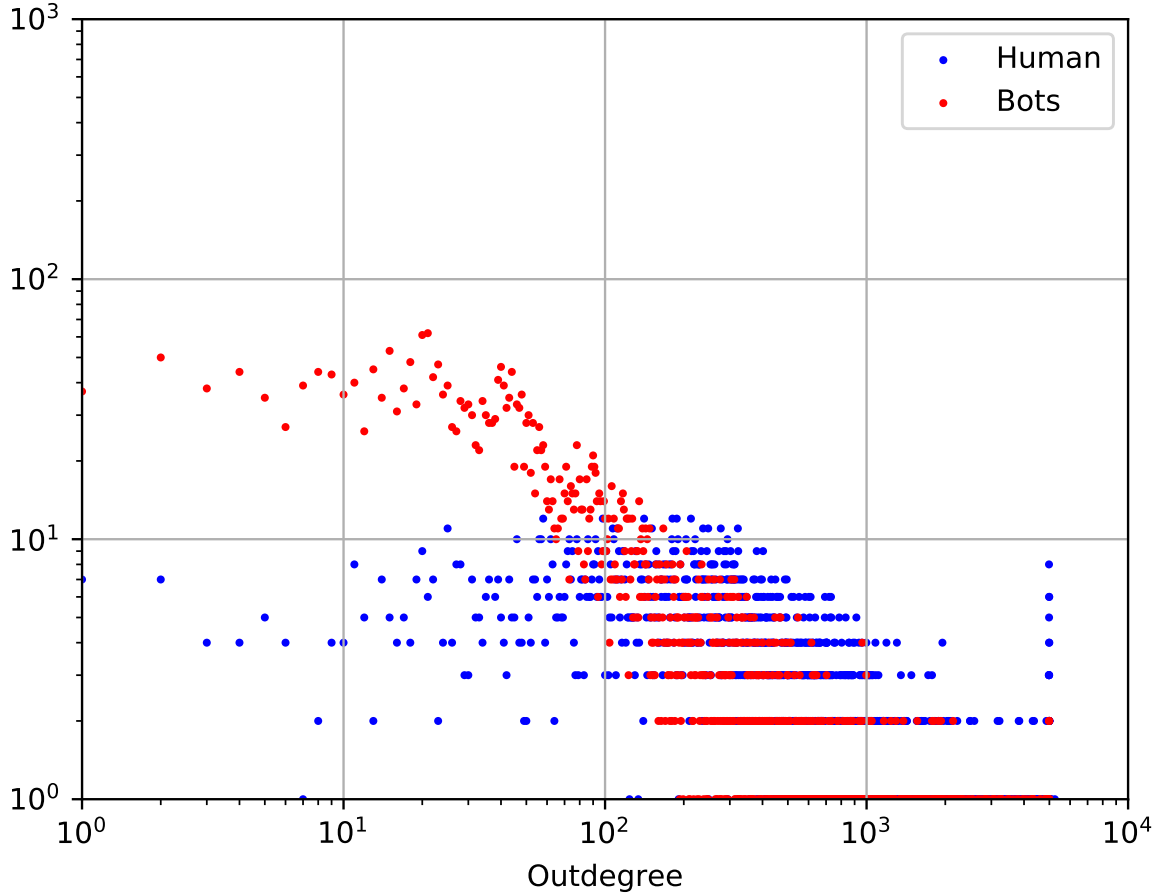
Connected components: 1,244

Social graph



Social graph





Social graph

Real users:

median in-degree 166

median out-degree 202

mean in-degree 576.8

mean out-degree 503.2

Bot accounts:

median in-degree 18

median out-degree 24

mean in-degree 113.7

mean out-degree 163.2

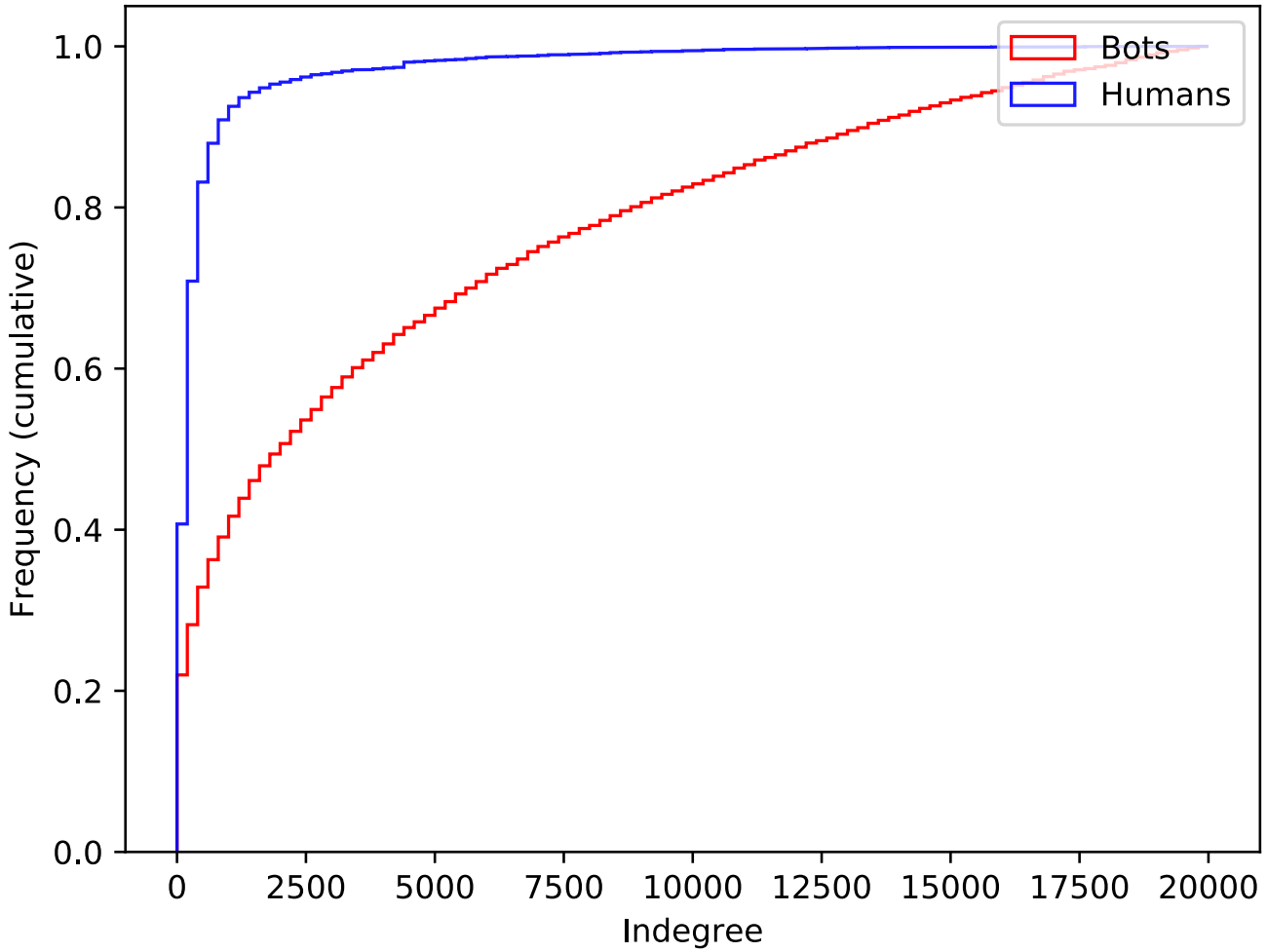
Social graph

Some bot accounts have many followers (and some follow many users).

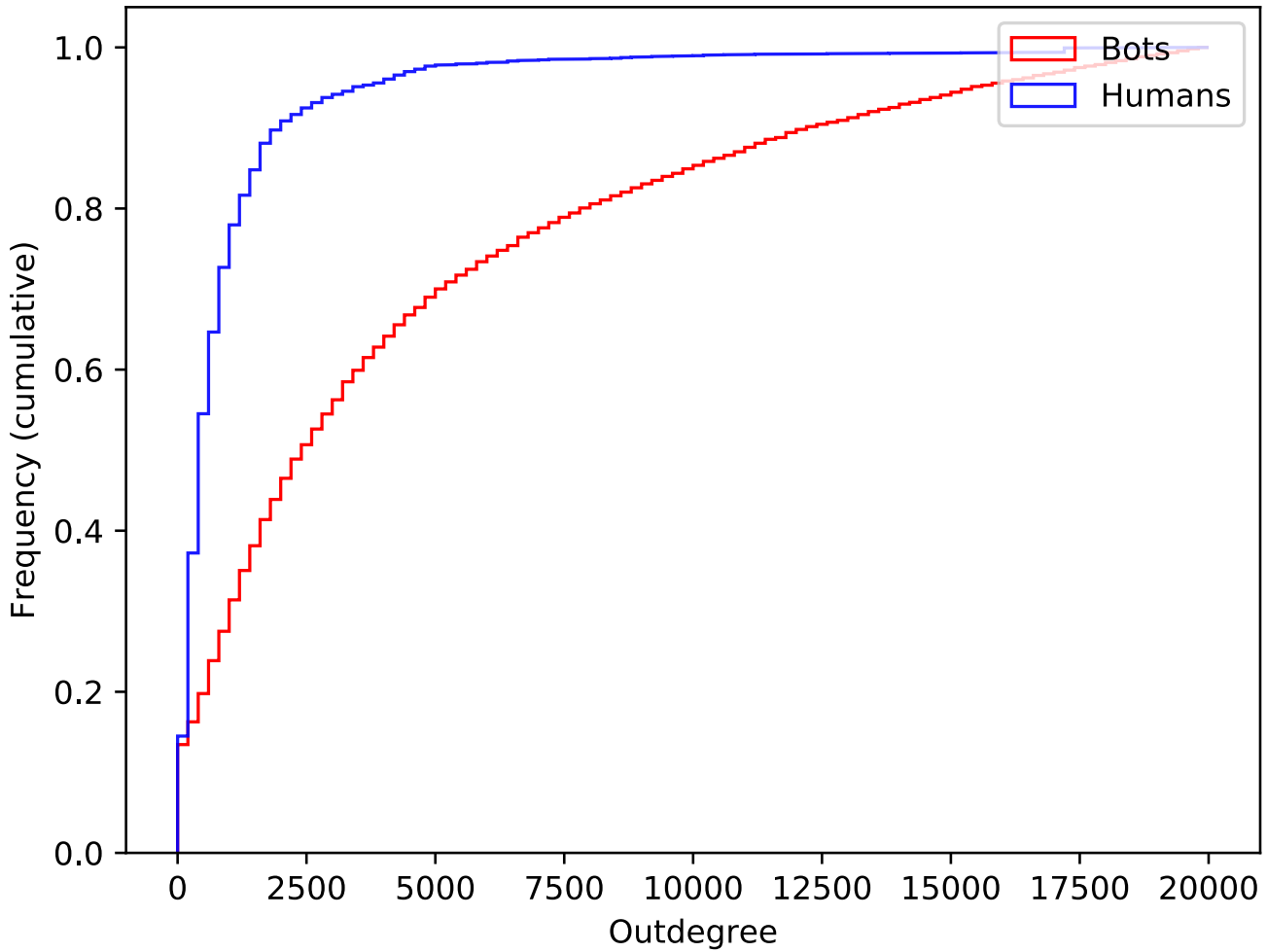
Also: bot accounts are more likely to be followed by other bots.

Classify accounts by looking their neighbors!

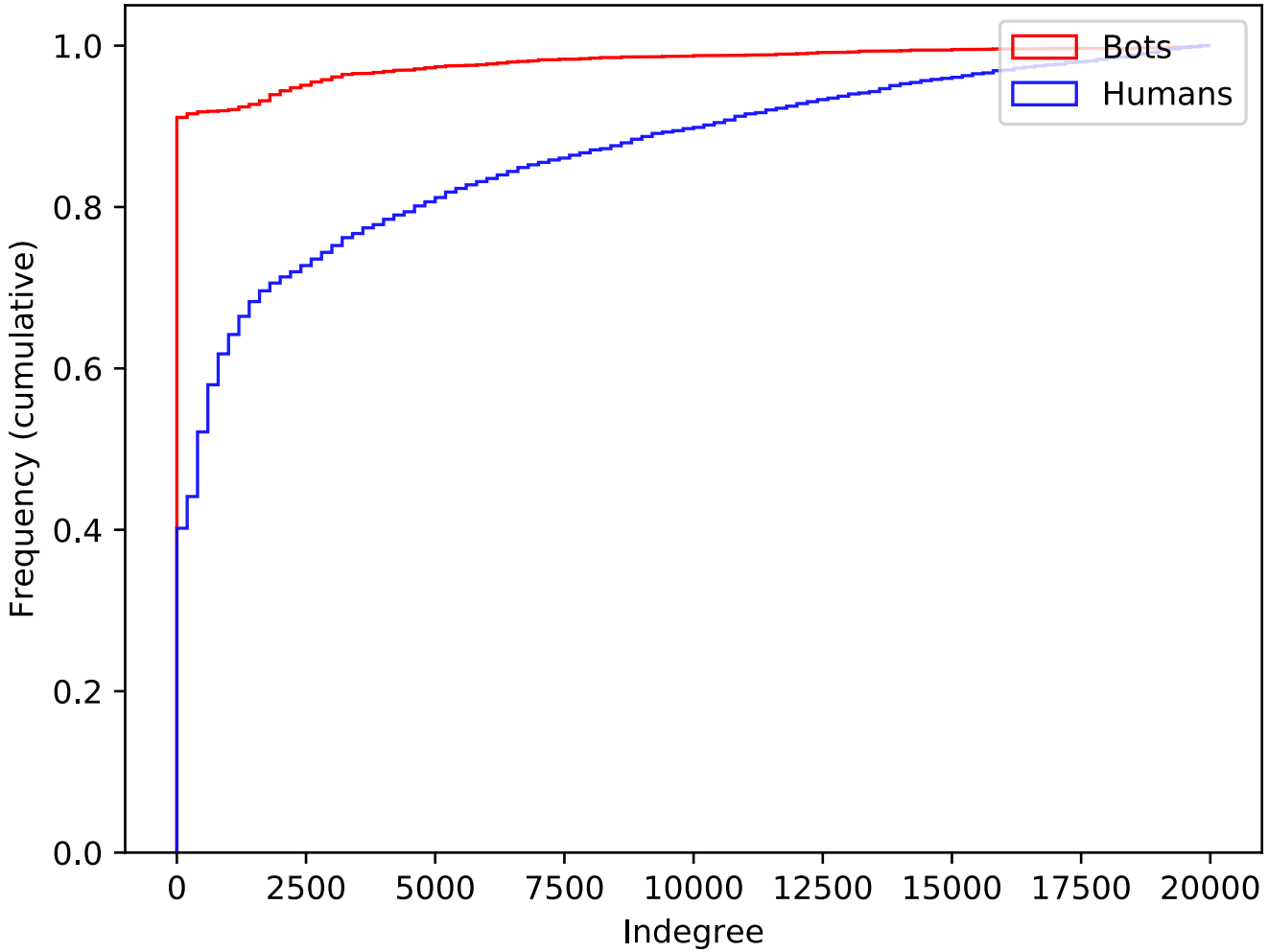
Median indegree of predecessors



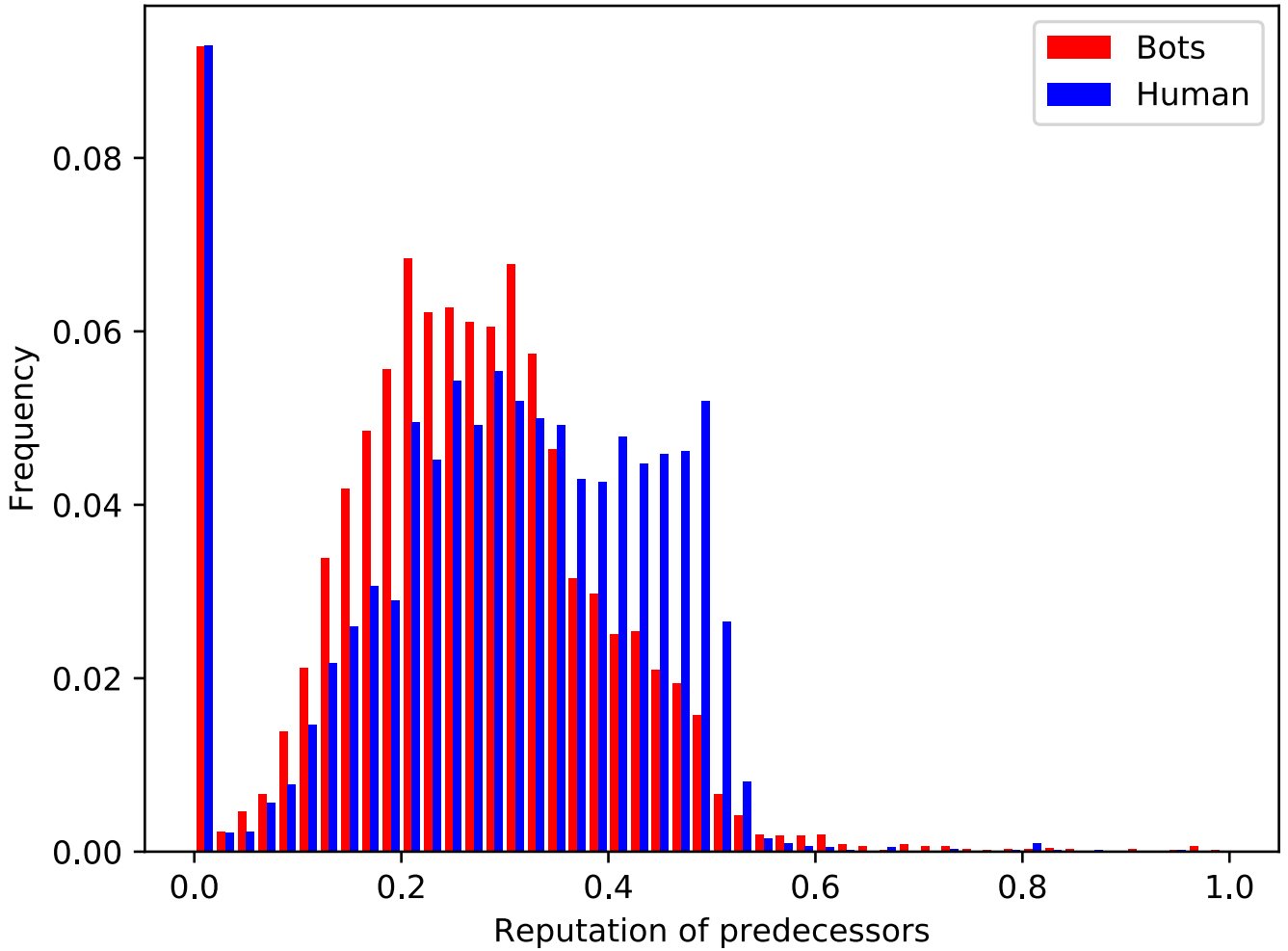
Median outdegree of predecessors



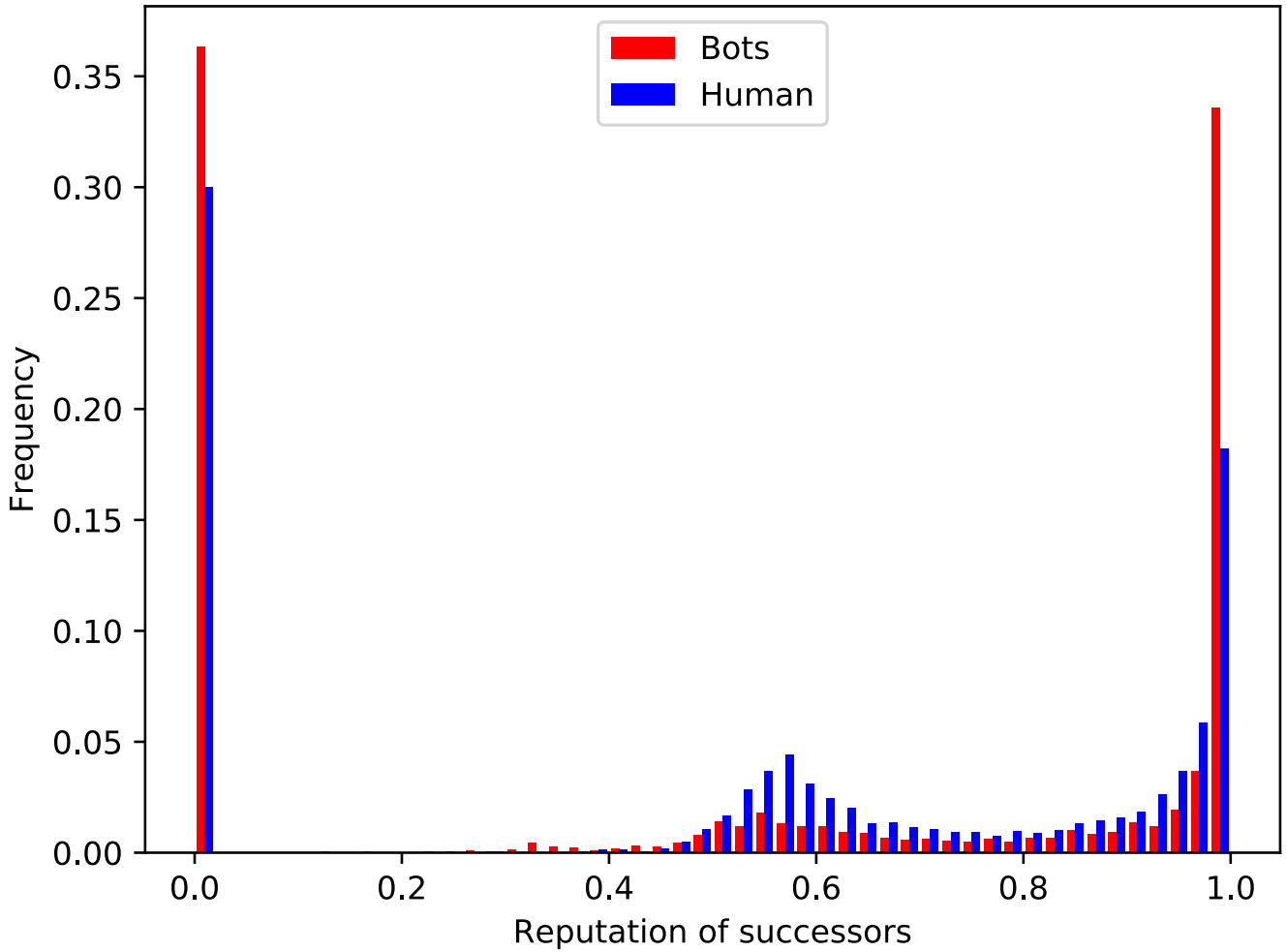
Median indegree successors



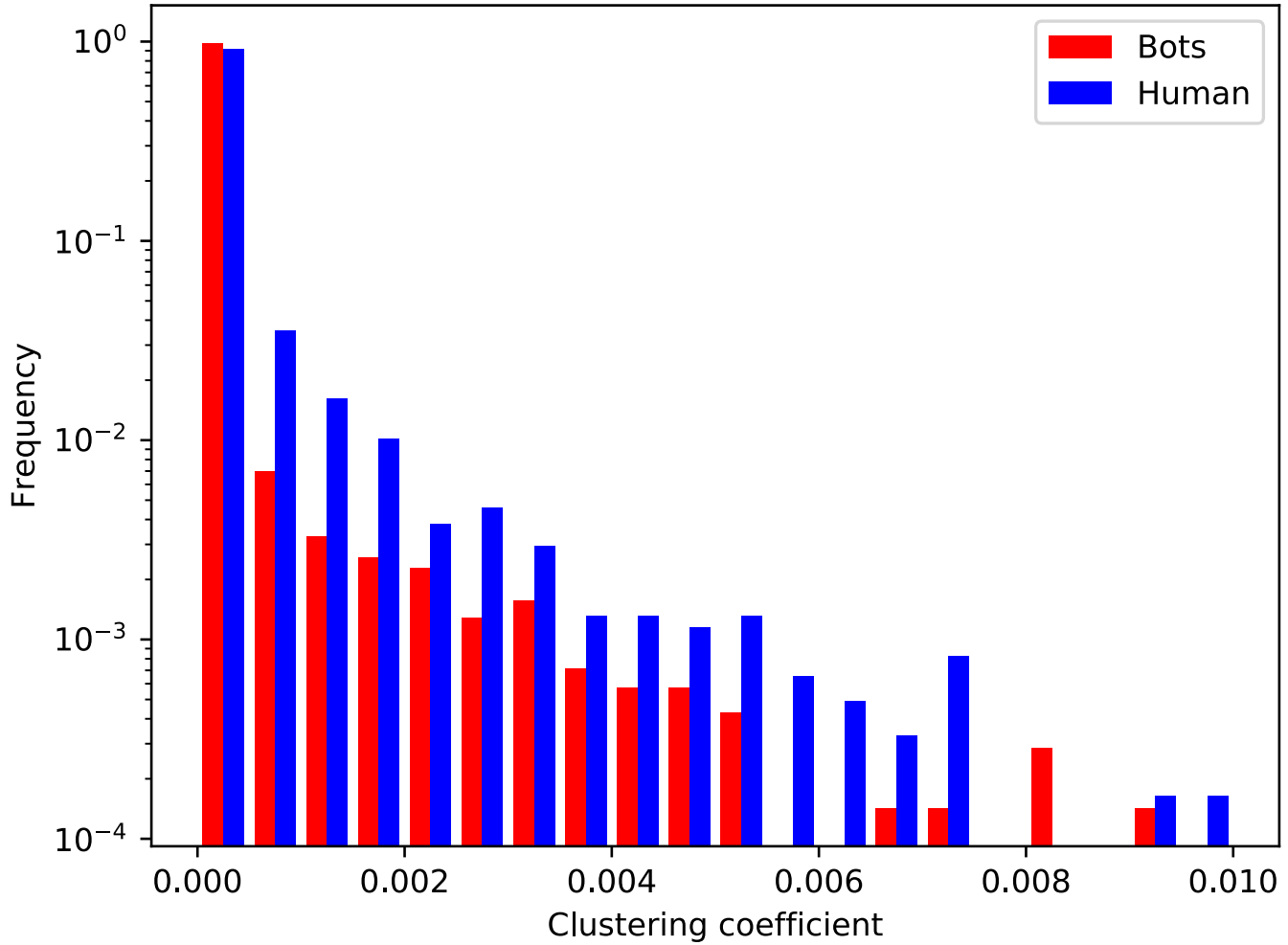
Reputation predecessors



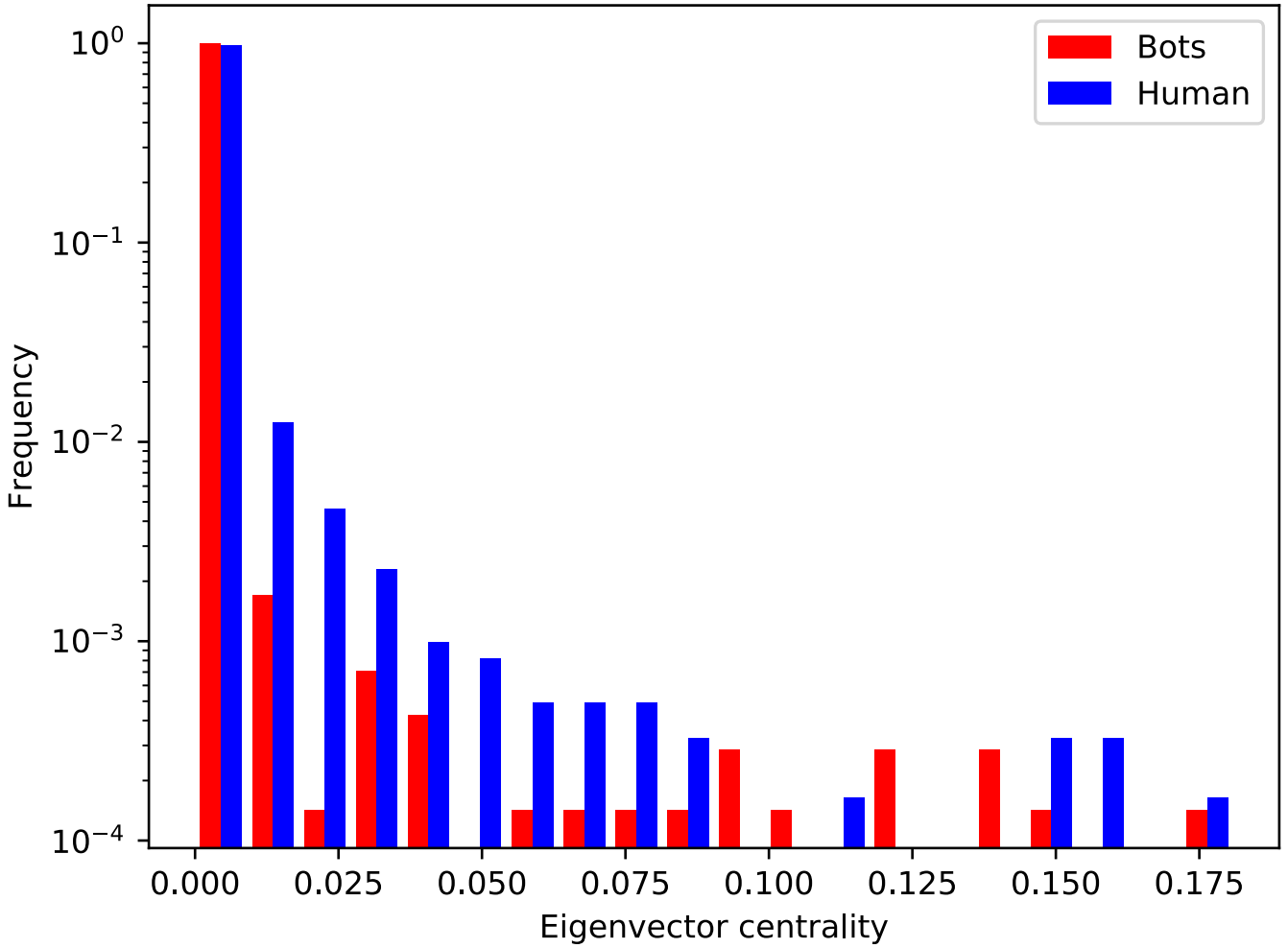
Reputation successors



Clustering coefficient



Eigenvector centrality



Proposed method

Observation: Fake accounts and bots don’t have the same social structure (and graph structure) as real users.

Proposed method

Idea: we can use

1. features of neighbors of each node
2. graph features
3. general graph topology

to find communities of fake accounts and aid fake account detection.

Proposed method

Features include:

- centrality measures
- degree
- reputation = followers/(following+followers)
- density
- clustering coefficient
- neighborhood-aggregated measures
- regular profile features

Proposed method

Next steps:

1. Run more experiments on the data [Nagmat, 15hrs]
2. Develop a classification method based on our findings [Both, 20hrs]
3. Evaluate our method and compare it to other approaches [Both, 30hrs]