

TwiBot-20: A Comprehensive Twitter Bot Detection Benchmark

Shangbin Feng
Xi'an Jiaotong University
Xi'an, China
wind_binteng@stu.xjtu.edu.cn

Herun Wan
Xi'an Jiaotong University
Xi'an, China
wanherun@stu.xjtu.edu.cn

Ningnan Wang
Xi'an Jiaotong University
Xi'an, China
mrwangyou@stu.xjtu.edu.cn

Jundong Li
University of Virginia
Charlottesville, USA
jundong@virginia.edu

Minnan Luo
Xi'an Jiaotong University
Xi'an, China
minnluo@xjtu.edu.cn

ABSTRACT

Twitter has become a vital social media platform while an ample amount of malicious Twitter bots exist and induce undesirable social effects. Successful Twitter bot detection proposals are generally supervised, which rely heavily on large-scale datasets. However, existing benchmarks generally suffer from low levels of user diversity, limited user information and data scarcity. Therefore, these datasets are not sufficient to train and stably benchmark bot detection measures. To alleviate these problems, we present TwiBot-20, a massive Twitter bot detection benchmark, which contains 229,573 users, 33,488,192 tweets, 8,723,736 user property items and 455,958 follow relationships. TwiBot-20 covers diversified bots and genuine users to better represent the real-world Twittersphere. TwiBot-20 also includes three modals of user information to support both binary classification of single users and community-aware approaches. To the best of our knowledge, TwiBot-20 is the largest Twitter bot detection benchmark to date. We reproduce competitive bot detection methods and conduct a thorough evaluation on TwiBot-20 and two other public datasets. Experiment results demonstrate that existing bot detection measures fail to match their previously claimed performance on TwiBot-20, which suggests that Twitter bot detection remains a challenging task and requires further research efforts.

1 INTRODUCTION

Twitter is one of the most popular social media platforms and as reported by Statista¹, where millions of daily active Twitter users use the platform. Twitter is also free to use and easy to access, which encourages individuals as well as organizations to view and publish contents of interests. Besides being used by genuine users, Twitter is home to an ample amount of automated programs, which are also known as Twitter bots. Some Twitter bots exploit Twitter features to pursue malicious goals such as election interference [10, 11] and extreme propaganda [2]. Twitter bots co-exist with human users on Twitter and they hide their automated nature by imitating genuine users. Since identifying bots in social media is crucial to preserving the integrity of the online discourse and these proposals are generally supervised, many research efforts have been devoted to the creation of relevant datasets.

Through the past decade, many bot detection datasets have been proposed and used. Regarding the user composition of datasets, the probots [31] dataset contains only Twitter bots where bot detection is treated as a task of outlier detection, while a majority

of datasets, such as varol-icwsm [27] and cresci-17 [6], contains both human and bot users to form a binary classification problem. Regarding user information, while caverlee [15] provides semantic and property information of Twitter users, gilani-17 [13] and others only include property information, and they vary greatly in user information completeness. Regarding dataset size, the number of users included in each dataset also range from 693 users in cresci-rtbust [19] to 50,538 in midterm-18 [32], and one of the most widely used dataset cresci-17 [6] contains 2,764 human users and 7,049 bots.

While previous research efforts have provided an ample amount of bot detection datasets for training and evaluation, they generally suffer from the following issues and fail to present a stable benchmark:

- **User diversity.** Existing bot detection datasets often focus on a specific type or cluster of users, failing to capture diversified bots that co-exist on the real-world Twittersphere. For example, dataset midterm-18 [32] only contains users that are actively involved in the 2018 US midterm elections. As a result, it fails to evaluate existing methods' ability to identify bots outside politics.
- **Limited user information.** Twitter users possess semantic, property and neighborhood information, while existing benchmarks only include a small fraction of multi-modal user information and fall short of comprehensiveness. For instance, the widely adopted cresci-17 [6] only contains semantic and property information, failing to incorporate user neighborhood information to support community-based bot detection approaches.
- **Data scarcity.** Previous small-scale datasets are not sufficient to train and stably benchmark novel bot detection measures, hindering the development of new approaches. To the best of our knowledge, the largest existing bot detection dataset midterm-18 [32] contains 50,538 users, leaving increasingly complex bot detectors data-hungry.

In light of the drawbacks of previous bot detection datasets, we collect and annotate a comprehensive Twitter bot detection benchmark TwiBot-20, which can alleviate the lack of user diversity, limited user information and data scarcity problems:

- We conduct BFS-based traversal through follow relationships, starting from a large number of seed users in different topics. As a result, users in TwiBot-20 are diverse in geographical locations and interest domains, making TwiBot-20 more representative of the current Twittersphere.

¹<https://www.statista.com/>

- We retrieve all three modals of user information, namely semantic, property and neighborhood information from Twitter API to facilitate leveraging multi-modal user information. To the best of our knowledge, TwiBot-20 is the first publicly available bot detection dataset that includes user follow relationships.
- To the best of our knowledge, TwiBot-20 establishes the largest benchmark of Twitter bot detection to date, which contains 229,573 Twitter users, 8,723,736 user property items, 33,488,192 tweets and 455,958 follow links.

In the following, we first review related work in Section 2, then define the task of Twitter bot detection in Section 3. We detail the collection and annotation process of TwiBot-20 in Section 4 and conduct in-depth data analysis in Section 5. We conduct extensive experiments to evaluate existing bot detection measures on TwiBot-20 in Section 6, and conclude the paper in Section 7.

2 RELATED WORK

In this section, we briefly review the related literature in social media bot detection and Twitter bot detection datasets.

2.1 Social Media Bot Detection

The first generation of proposals for Twitter bot detection focuses on feature engineering with user information. Lee *et al.* [17] proposed to verify URL redirections in tweets. Thomas *et al.* [26] focused on classifying mentioned websites. Gao *et al.* [12] merges spam tweets into campaigns for bot detection. Yang *et al.* [30] designed novel features to counter the evolution of Twitter bots. Other features are also adopted such as information on the user homepage [16], social networks [22], and timeline of accounts [5].

With the advent of deep learning, neural networks are increasingly adopted for Twitter bot detection. Stanton *et al.* [25] leveraged generative adversarial networks for Twitter bot detection. Wei *et al.* [29] used recurrent neural networks to identify bots with tweet semantics. Kudugunta *et al.* [14] jointly leveraged user features and tweet semantics to propose a LSTM-based bot detector. Alhosseini *et al.* [1] proposed to adopt graph convolutional networks to leverage user features and the Twittersphere structure.

2.2 Twitter Bot Detection Datasets

An ample amount of datasets are proposed to train and evaluate bot detection methods. One of the earliest bot detection dataset is caverlee-2011 [16], which is collected from December 30, 2009 to August 2, 2010 on Twitter with 22,223 content polluters and 19,276 legitimate users. Another early dataset is cresci-2015 [4] which provides a dataset of genuine accounts and fake followers.

An increasing amount of bot detection benchmarks are proposed since 2017. varol-2017 [28] contains manual annotation of 2,573 Twitter accounts. vendor-purchased-2019 [31] consists of fake follower accounts purchased online. To the best of our knowledge, the largest Twitter bot detection dataset to date is midterm-18 [32], providing 50,538 annotated users. Apart from that, verified-2019 [32], botwiki-2019 [32], cresci-rtbust-2019 [20], Astroturf [24] are also more recent bot detection datasets of various size and information completeness.

Algorithm 1: TwiBot-20 User Selection Strategy

```

Input: initial seed user  $u_0$  in a user cluster
Output: user information set  $F$ 

 $u_0.layer \leftarrow 0$ ; // designate seed user as layer 0
 $S \leftarrow \{u_0\}$ ; // set of users to expand
 $u_0.expanded \leftarrow False$ ;
 $F \leftarrow \emptyset$ ;
while  $S \neq \emptyset$  do
     $u \leftarrow S.pop()$ ; // expand with user  $u$ 
     $T(u) \leftarrow get\_tweet(u)$ ;
     $P(u) \leftarrow get\_property(u)$ ;
    if  $u.layer \geq 3$  or  $u.expanded == True$  then
         $F \leftarrow F \cup u(T, P, N = \emptyset)$ ;
        continue; // three layers max
     $u.expanded \leftarrow True$ ;
     $N^f(u) \leftarrow get\_friend(u)$ ;
     $N^t(u) \leftarrow get\_follower(u)$ ;
     $N(u) \leftarrow \{N^f(u), N^t(u)\}$ ;
     $F \leftarrow F \cup u(T, P, N)$ ;
     $S \leftarrow S \cup N^f(u) \cup N^t(u)$ ;
    for  $y \in N^f(u) \cup N^t(u)$  do
         $y.expanded \leftarrow False$ ;
         $y.layer \leftarrow u.layer + 1$ ;

```

Return F ; // obtained one cluster of user information

3 PROBLEM DEFINITION

A Twitter bot is a type of bot software that controls a Twitter account via automated programs and the Twitter API. In this paper, we study the problem of Twitter bot detection to identify Twitter bots that pursue malicious goals since they pose threat to the online discourse.

Let U be a Twitter user, consisting of three aspects of user information: semantic T , property P and neighborhood N . Semantic information of Twitter users are user-generated natural language posts and texts, such as tweets and replies. Property information of Twitter users are numerical and categorical user features such as follower count and whether the user is verified. Neighborhood information of Twitter users are their followers and followings, which form the graph structure of the Twittersphere. Similar to previous research [14, 32], we treat Twitter bot detection as a binary classification problem, where each user could either be human ($y = 0$) or bot ($y = 1$).

Formally, we can define the Twitter bot detection task as follows. Given a Twitter user U and its information T , P and N , learn a bot detection function $f : f(U(T, P, N)) \rightarrow \hat{y}$, such that \hat{y} approximates ground truth y to maximize prediction accuracy.

4 DATA COLLECTION

In this section, we present how to select Twitter users from the Twittersphere, retrieve multi-modal user information and derive trustworthy annotations to construct the benchmark. TwiBot-20 was collected in this way from July to September 2020.

4.1 User Selection Strategy

To diversify user sampling in order to better approximate the current Twittersphere, TwiBot-20 employs breadth-first search starting from different root nodes, which is named seed users in our algorithm. Specifically, we treat users on the Twittersphere as nodes and their follow relationship as edges to form a directed graph. For each seed user, it is placed in layer 0 of that user cluster. Users in layer $i + 1$ are expanded from users in layer i along their follow edges. Such an expansion process ends at layer 3 and forms a user cluster. TwiBot-20 merges user clusters starting from different seed users to form the complete dataset. TwiBot-20’s user selection strategy is presented in Algorithm 1, following notations defined in Section 3.

TwiBot-20’s user selection strategy is different from previous benchmarks in that it does not demand selected users to follow any given pattern or restrict them to any specific topic. Such a relaxation of constraints is crucial for TwiBot-20 to better represent the diversified Twittersphere and evaluate bot detectors’ ability to capture multiple types of bots that co-exist on online social media.

4.2 Seed User Selection

As detailed in Section 4.1, TwiBot-20 is obtained by controlled breadth-first search expanded from different seed users. The goal of TwiBot-20 is to accurately represent the diversified Twittersphere to benchmark generalizable bot detection, thus the search algorithm should be designed to cover diverse user groups and communities. Politics, business, entertainment and sports are four interest domains that would overlap with everyone’s online engagements. Thus, unlike previous bot detection datasets which are limited to a specific topic or hashtag, TwiBot-20 selects diverse seed users from these domains to result in a representative collection of the current Twittersphere. Specifically, 40 seed users come from these four distinct disciplines:

- Politics: We select national and local politicians from diverse ideological spectrum, major media outlets and influential political commentators as seed users. e.g. @SpeakerPelosi
- Business: We select corporations, financial media outlets and influential business pundits as seed users. e.g. @amazon
- Entertainment: We select well-known artists, comedians and video game streamers as seed users. e.g. @samsmith
- Sports: We select athletes, sports team and sports news outlets from various types of sports as seed users. e.g. @StephenCurry30

In addition to the big names in each area, we also sample users who comment under relevant tweets and active users in relevant hashtags as seed users to provide another view of the community and ensure exhaustiveness. A complete list of all seed users is available in the full dataset TwiBot-20. By using a large number of seed users from different interest domains, we ensure that TwiBot-20 covers diversified users to better represent the current Twittersphere.

4.3 User Information Selection

After determining the user list of TwiBot-20, we use Twitter API to retrieve all three aspects of user information as defined in Section 3. Specifically,

- For semantic information, we retrieve the most recent 200 tweets of each Twitter user to capture its recent activities. We preserve the original form of the multilingual tweet content, leaving emojis, urls and retweets intact for bot detectors to process tweet text in ways they see fit.
- For property information, we incorporate all property items provided by the Twitter API for each user. As a result, each user has 38 property items recorded in TwiBot-20.
- For neighborhood information, we retrieve followers and followings of a Twitter user and record follow relationships between users in TwiBot-20.

Existing bot detection datasets mostly leave out neighborhood information and contains only a fraction of property items or user tweets. In comparison, TwiBot-20 includes all user information that is directly retrievable from the Twitter API so that future bot detectors could leverage whatever user information they see fit without being constrained by the scope of the dataset.

4.4 Data Annotation Strategy

Data annotation in Twitter bot detection is particularly difficult and prone to bias, thus we employ a specialized data annotation strategy that draws on conclusions of previous research efforts and emphasize trustworthiness. Firstly, we summarize previous literature and propose general criteria to identify a bot user, which are listed as follows:

- Lack of pertinence and originality in tweets.
- Highly automated activity and API usage.
- Tweets containing external link promoting phishing or commercials.
- Repeated tweets with identical content.
- Tweets containing irrelevant URLs.

Guided by these standards, we launch a crowdsourcing campaign at Appen². According to our contract, annotators should be active Twitter users and are required to read a guidelines document in which we explain the five characteristics of bots along with representative examples. Five annotators are then assigned to each user in TwiBot-20 to determine whether it is operated by bot or not. In order to identify potentially ambiguous cases, annotators are permitted to report ‘undecided’ regarding a specific user. We also designed standard questions where the user is clearly a bot or human. We mix these standard questions with annotation inquiries to evaluate an annotator’s performance. Annotators who are more than 80% correct on standard questions are considered to be trustworthy and their annotation is adopted. As a result, the crowdsourcing campaign provided 63,816 annotation records and takes approximately 33 days.

Although we provided annotation guidelines, assigned five annotators to each user and designed standard questions for performance evaluation, the crowdsourcing results are not reliable on its own. We further take the following steps to reach the final annotation of users in TwiBot-20:

- Firstly, if a user is verified by Twitter, we consider it to be a genuine user.

²<https://www.appen.com/>

Table 1: Statistics of different bot detection benchmarks, from left to right, user count, user property item count, total tweet count and follow relationship count in each dataset.

Dataset	#User	#Property	#Tweet	#Follow
varol-icwsm [27]	2,573	0	0	0
pronbots [31]	21,965	750,991	0	0
celebrity [31]	5,971	879,954	0	0
gilani-17 [13]	2,653	104,515	0	0
cresci-rtbust [19]	693	28,968	0	0
cresci-stock [7]	13,276	551,603	0	0
midterm-18 [32]	50,538	909,684	0	0
botwiki [32]	698	29,082	0	0
verified [32]	1,987	83,383	0	0
PAN-19 ³	11,568	0	369,246	0
caverlee [15]	22,224	155,568	5,613,166	0
cresci-17 [6]	14,398	547,124	18,179,186	0
TwiBot-20	229,573	8,723,736	33,488,192	455,958

- For remaining users, if four out of five annotators believe that it is bot or human, we annotate the user accordingly.
- For other users with less mutual agreement from crowdsourcing, we use Twitter’s direct message feature to send out simple questions in natural language, collect answers from users that respond and manually determine their annotations.
- Finally, remaining undecided users are manually examined within our research team. To ensure the trustworthiness of these ambiguous users, we discard disputed cases and only annotate when we reach a consensus on a Twitter user.

Data annotation in Twitter bot detection is heavily influenced by underlying assumptions and subject to bias. We synthesize previous literature, launch a carefully designed crowdsourcing campaign and follow a meticulous process to reach the final annotation of a specific user. Further analysis in Section 5.4 would further demonstrate the trustworthiness of TwiBot-20 annotations.

4.5 Data Release

Users in TwiBot-20 are determined in Section 4.1 and Section 4.2. Multi-modal user information is retrieved from Twitter API as described in Section 4.3 and Section 4.4 details how we created trustworthy annotations for TwiBot-20. We release these data according to the following process:

- We conduct a random partition of 7:2:1 on the labeled users to obtain the train, validation and test set of the TwiBot-20 benchmark. In order to preserve the dense graph structure follow relationship forms, we also provide unsupervised users as the support set of TwiBot-20.
- We organize users in each set into the JSON format to obtain four data files: `train.json`, `dev.json`, `test.json` and `support.json`. For each user, we provide user IDs to identify users and all their semantic, property and neighborhood information collected in Section 4.3.
- We release TwiBot-20 with succinct documentation at <https://github.com/BunsenFeng/TwiBot-20>. A small sample of TwiBot-20 is directly available at the github repository, while researchers

Table 2: User information modalities that each bot detection dataset contains. The definition of semantic, property and neighborhood information follows that of Section 3. varol-icwsm [27] is considered to not contain any aspect of user information since it is merely a list of user ids that are considered to be bots or human.

Dataset	Property	Semantic	Neighbor
varol-icwsm [27]			
pronbots [31]		✓	
celebrity [31]		✓	
gilani-17 [13]		✓	
cresci-rtbust [19]		✓	
cresci-stock [7]		✓	
midterm-18 [32]		✓	
botwiki [32]		✓	
verified [32]		✓	
PAN-19 ³			✓
caverlee [15]		✓	✓
cresci-17 [6]		✓	✓
TwiBot-20	✓	✓	✓

are also encouraged to download and use the full TwiBot-20 to facilitate bot detection research.

5 DATA ANALYSIS

In this section, we firstly contrast the size of different bot detection datasets. We then compare TwiBot-20’s information completeness and user diversity with other benchmarks. Finally we conduct annotation analysis to demonstrate the trustworthiness of TwiBot-20 annotations.

5.1 Dataset Size Analysis

Bot detection on social media focuses on solving the real-world problem of online bot presence. In order to well represent real-world genuine users and Twitter bots, a bot detection dataset should be considerable in size to achieve such purpose. We contrast TwiBot-20 and major bot detection datasets regarding dataset size in Table 1.

Table 1 demonstrates that TwiBot-20 leads with a total of 229,573 users, significantly outnumbering previous bot detection datasets. TwiBot-20 also provides a support set that includes massive amount of unsupervised users. This support set enables novel trends such as semi-supervised learning to merge with bot detection research. To the best of our knowledge, TwiBot-20 establishes the largest bot detection benchmark to date and is the first to provide unsupervised users in a bot detection dataset.

5.2 User Information Analysis

Online social media is becoming increasingly complex, with users generating huge volumes of multi-modal data every day. Twitter bots are also leveraging this information complexity to evade previous bot detection measures. Twitter users often generate large volumes of multi-modal data, thus bot detection datasets should incorporate all three modals of user information to allow comprehensive analysis of user’s behaviour, which might boost bot

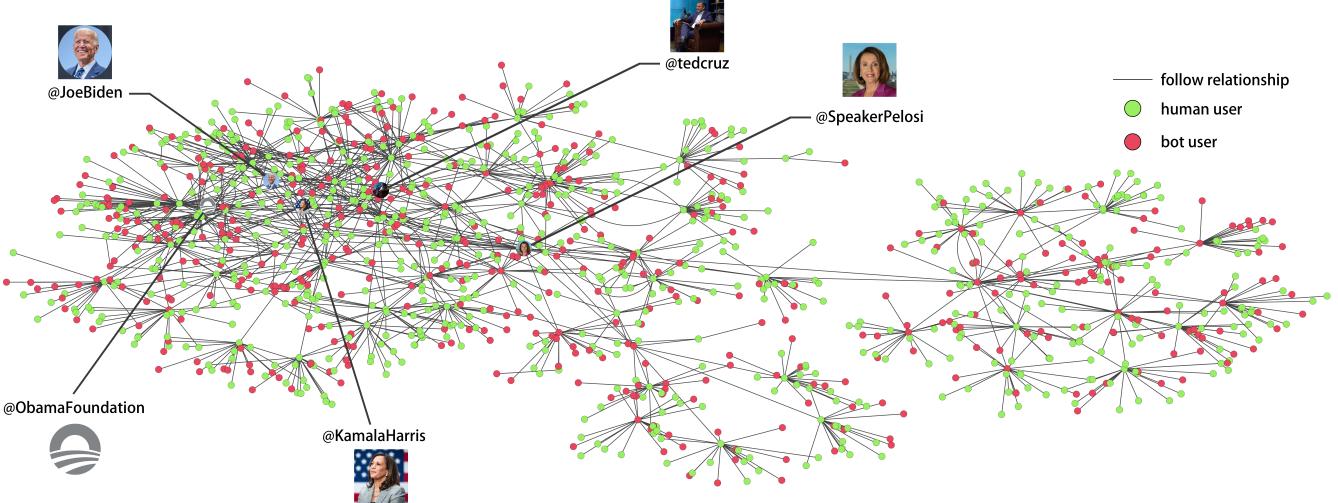


Figure 1: Illustration of a user cluster in TwiBot-20 with @SpeakerPelosi as the seed user. Green nodes represent human users in the user cluster, red nodes represent bot users and edges in the graph indicates that one user follows the other.

detection performance and robustness. We study major bot detection datasets and depict their user information completeness in Table 2.

Table 2 demonstrates that TwiBot-20 contains all three aspects of user information. Dataset cresci-17 [6] and caverlee [15] contain both semantic and property information, while all other existing baselines only include user semantic or property information. Further exploration shows that datasets with only property information often leaves out certain property items, introducing inevitable bias in the process. To the best of our knowledge, TwiBot-20 is the first publicly available Twitter bot detection benchmark that incorporates user neighborhood information. TwiBot-20’s information completeness enables novel bot detectors to leverage as much user information as it could be explicitly retrieved.

To further explore TwiBot-20’s user neighborhood information, we illustrate a cluster of users in TwiBot-20 and their follow relationship in Figure 1. It is demonstrated that follow relationship in TwiBot-20 forms a dense graph structure to enable community-based bot detection measures such as graph neural networks.

5.3 User Diversity Analysis

An important aim of TwiBot-20 is to accurately represent the diversified Twittersphere and capture different types of bots that co-exist on social media. We study the distribution of profile locations and user interests to examine whether TwiBot-20 has achieved the goal of user diversity.

Geographic diversity. Figure 2 illustrates the geographic location of users in TwiBot-20. While the most frequent two countries are India and the United States, there are also a considerable amount of users from Europe and Africa.

User interest diversity. Figure 3 illustrates the most frequently mentioned hashtags and their frequency. The #COVID19 hashtag ranks first due to the global health crisis at the time of data collection. It is demonstrated that TwiBot-20 captures political users

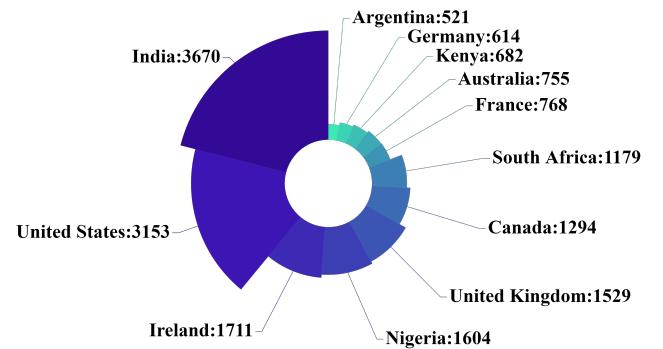


Figure 2: Most frequent countries of user location in TwiBot-20 and their number of appearances. There are 179 countries that appear less than 500 times and they collectively appear 11835 times in TwiBot-20, which are omitted in the figure to preserve clarity.

that often tweet with #Trump and #RNC2020, sports lovers with #SaintsFC, business people with #business and #marketing, as well as ordinary users that tweet with #love and #travel.

Twitter users in TwiBot-20 are thus proved to be diversified in geographic locations and interest domains. TwiBot-20 contains diversified users to better represent the diversified Twittersphere rather than being toy examples of specific scenarios.

5.4 Annotation Quality Analysis

To prove that our annotation procedure leads to high quality annotation, we examine whether the annotation results are consistent with bot characteristics proposed in previous literature.

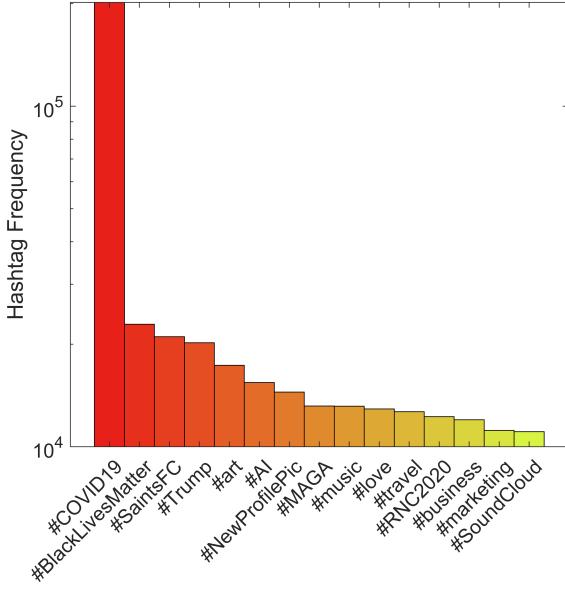


Figure 3: Most frequent hashtags in user tweets in our proposed TwiBot-20. We merge similar hashtags such as #COVID19 and #coronavirus and select the 15 hashtags of highest frequency.

Account Reputation. We explore the difference between the reputation score [3] of bot and genuine users in TwiBot-20. Reputation is a coefficient that measures a user’s follower count and friend count, defined as follows:

$$Reputation(u) = \frac{|N^t(u)|}{|N^t(u)| + |N^f(u)|} \quad (1)$$

where $|\cdot|$ denotes the cardinality of a set, $N^t(u)$ denotes the follower set of user u and $N^f(u)$ denotes the following set of user u .

Chu *et al.* [3] observed that, human users are more likely to follow “famous” or “reputable” users. A celebrity usually has many followers and few friends, and his reputation is close to 1. In contrast, for a bot with few followers and many friends, its reputation is close to 0. We illustrate the cumulative distribution function (CDF) of account reputation for bot and human users in Figure 4(a). It is illustrated that genuine users in TwiBot-20 exhibit relatively higher reputation score than bots. Around 60 percent of bots in TwiBot-20 have fewer followers than friends, causing their reputation to be less than 0.5. The reputation score of users in TwiBot-20 matches the proposal of Chu *et al.* [3], which strengthens the claim that TwiBot-20 annotation is generally trustworthy.

User Tweet Count. Perdana *et al.* [23] observed that bot users would generate a lot of repeated tweets, leading to a higher total tweet count. We explore the relationship between user annotation and its tweet count in TwiBot-20. Figure 4(b) shows the CDF of user tweet counts. It is surprising that bot users generate fewer tweets than human. This discrepancy with previous work could be attributed to the fact that bot users have evolved to escape feature-engineering based bot detection and they control the number of

tweets now. To further explore this difference, we check the bot users in our dataset and find out the following fact: bot users tweet more frequently in a certain period with long-term hibernation to avoid detection by Twitter, which results in fewer tweets in general.

Screen Name Likelihood. Yang *et al.* [32] observed that bot users sometimes use a random string as their screen name. To measure this feature, they proposed to evaluate the screen name likelihood of users. Twitter only allows letters (upper and lower case), digits and underscores in the screen name field with a 15-character limit. We use the 229,573 screen names in TwiBot-20 and construct the likelihood of all 3,969 possible bigrams. The likelihood of a screen name is defined by the geometric-mean likelihood of all bigrams in it. For a screen name X with length k , the likelihood $L(x)$ is defined as follows:

$$L(x) = \left[\prod_{i=1}^{k-1} P(x_i, x_{i+1}) \right]^{\frac{1}{k-1}} \quad (2)$$

where x_i denotes the i -th character of X and $P(x_i, x_{i+1})$ denotes the likelihood of bigram (x_i, x_{i+1}) obtained from the user screen names.

Figure 4(c) illustrates the difference between bot users and human users in screen name likelihood. The results indicate that bot users in TwiBot-20 do have slightly lower screen name likelihood, which is compatible with the findings in Yang *et al.* [32]. We examine some bot users and find that they do have random strings as their screen name such as @Abolfaz54075615. Data annotation in TwiBot-20 also matches Yang *et al.* [32]’s observation, which lends support to TwiBot-20’s annotation credibility.

To sum up, TwiBot-20’s annotation generally matches previously proposed bot characteristics.

6 EXPERIMENTS

In this section, we conduct extensive experiments and in-depth analysis on TwiBot-20 and two other public datasets to prove the novelty and effectiveness of the proposed benchmark.

6.1 Experiment Settings

Datasets. In addition to our proposed benchmark TwiBot-20, we make use of two other publicly available datasets cresci-17 [6] and PAN-19³ to compare baseline performance on different benchmarks.

cresci-17 [6] is partitioned into genuine users, social spam bots, traditional spam bots and fake followers. We utilize cresci-17 as a whole. As of user information, cresci-17 contains semantic and property information of Twitter users.

PAN-19³ is a dataset of a Bots and Gender Profiling shared task in the PAN workshop at CLEF 2019. It contains user semantic information.

A summary of these three datasets is presented in Table 3. For three datasets, We randomly conduct a 7:2:1 partition as training, validation, and test set. Such a partition is shared across all experiments in Section 6.2, 6.3, 6.4 and 6.5.

Baselines. We introduce competitive and state-of-the-art bot detection methods adopted in the experiments:

³<https://pan.webis.de/clef19/pan19-web/author-profiling.html>

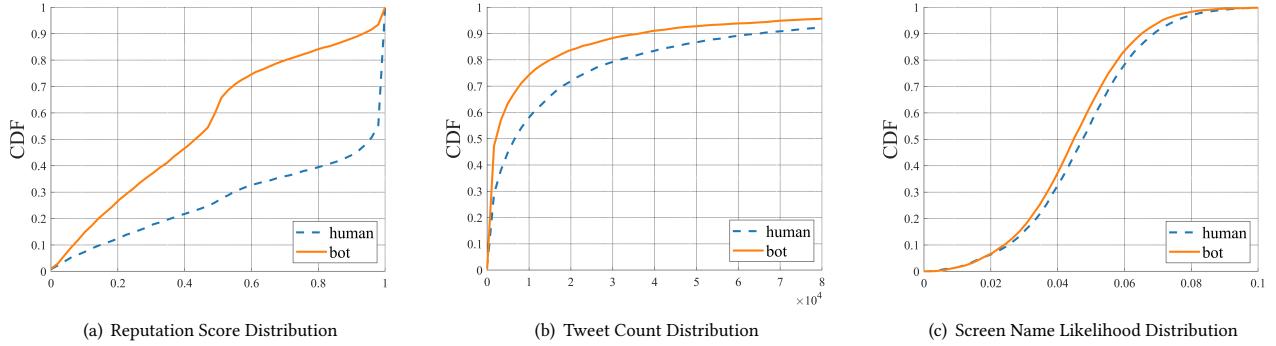


Figure 4: Cumulative distribution functions of reputation, tweet count and name likelihood among bots and genuine users.

Table 3: Overview of three adopted bot detection datasets. S, P and N info stands for semantic, property and neighborhood information respectively.

Dataset	User Count	Semantic Info	Property Info	Neighbor Info	Release Year
TwiBot-20	229,573	✓	✓	✓	2020
Cresci-17 [6]	9,813	✓	✓		2017
PAN-19 ³	11,378	✓			2019

- Lee *et al.* [16]: Lee *et al.* use random forest classifier with feature engineering.
- Yang *et al.* [32]: Yang *et al.* use random forest with user metadata and derived secondary features.
- Kudugunta *et al.* [14]: Kudugunta *et al.* propose to use LSTM and fully connected neural networks to jointly leverage tweet semantics and user metadata.
- Wei *et al.* [29]: Wei *et al.* use word embeddings and a three-layer BiLSTM to encode tweets and identify bots.
- Miller *et al.* [21]: Miller *et al.* use 107 features and modified stream clustering algorithm for bot detection.
- Cresci *et al.* [5]: Cresci *et al.* encodes user activities with strings and computes longest common substring to capture bot in groups.
- Botometer [9]: Botometer is a publicly available demo that leverages more than one thousand features to identify Twitter bots on demand.
- Alhosseini *et al.* [1]: Alhosseini *et al.* adopt graph convolutional network for bot detection.

Evaluation Metrics. We adopt Accuracy, F1-score and MCC [18] as evaluation metrics. Accuracy is a straightforward metric while F1-score and MCC are more balanced alternatives.

6.2 Benchmark performance

Table 4 reports bot detection performance of different methods on two public datasets cresci-17, PAN-19³ and our proposed TwiBot-20. Table 4 demonstrates that:

- All bot detection baselines achieve significantly lower performance on TwiBot-20 than on cresci-17 or PAN-19³. This indicates that our TwiBot-20 is more challenging and social media bot detection is still an open problem.

- Alhosseini *et al.* [1] applies graph convolutional network to the task of Twitter bot detection, which demands that bot detection datasets include user neighborhood information. As Cresci *et al.* [8] points out, studying user communities is essential in future bot detection endeavors, where TwiBot-20 enables it by providing users’ neighborhood information and the two other datasets fall short.
- From the comparison between Wei *et al.* [29] and Kudugunta *et al.* [14], where both baselines use semantic information but the latter method also leverages user properties, it is demonstrated that the performance gap between two baselines is significantly larger on our proposed TwiBot-20 than on cresci-17. This indicates that apart from being a toy example, TwiBot-20 is relatively more complex, where bot detectors need to leverage more user information in order to perform well.
- Botometer [9] is a publicly available bot detection demo. Although it succeeds in capturing bots in cresci-17 where users in the dataset were collected back in 2017, it fails to match its previous performance on TwiBot-20, where users are collected in 2020. This demonstrates that the real-world Twittersphere has shifted and Twitter bots have evolved to evade previous detection methods, which calls for new research efforts and more up-to-date benchmarks like TwiBot-20.
- For feature engineering based methods such as Lee *et al.* [16] and Yang *et al.* [32], their performance drops significantly from cresci-17 to TwiBot-20. This trend indicates that failing to incorporate semantic and neighborhood information leads to worse performance on more recent datasets. This could again be attributed to the evolution of Twitter bots, thus future bot detection methods should leverage increasingly diversified and multi-modal user information to achieve desirable performance.

6.3 Dataset Size Study

TwiBot-20 contains more Twitter users than any other known bot detection dataset and covers more types of accounts compared with existing bot detection benchmarks. In this section, we analyze the benefits of the enlarged scale and the challenge of more diversified users. We randomly choose different proportions of users from the Twibot-20 training set and compare the model performances trained with different data sizes in Figure 5.

Table 4: The overall Twitter bot detection performance of various methods on our proposed TwiBot-20 and two public datasets, Cresci-17 [6] and PAN-19³. “/” denotes that the dataset doesn’t have sufficient user information to support the method.

		Lee <i>et al.</i> [16]	Yang <i>et al.</i> [32]	Kudugunta <i>et al.</i> [14]	Wei <i>et al.</i> [29]	Miller <i>et al.</i> [21]	Cresci <i>et al.</i> [5]	Botometer [9]	Alhosseini <i>et al.</i> [1]
TwiBot-20	Acc	0.7456	0.8191	0.8174	0.7126	0.4801	0.4793	0.5584	0.6813
	F1	0.7823	0.8546	0.7517	0.7533	0.6266	0.1072	0.4892	0.7318
	MCC	0.4879	0.6643	0.6710	0.4193	-0.1372	0.0839	0.1558	0.3543
Cresci-17	Acc	0.9750	0.9847	0.9799	0.9670	0.5204	0.4029	0.9597	/
	F1	0.9826	0.9893	0.9641	0.9768	0.4737	0.2923	0.9731	/
	MCC	0.9387	0.9625	0.9501	0.9200	0.1573	0.2255	0.8926	/
PAN-19³	Acc	/	/	/	0.9464	/	0.8797	/	/
	F1	/	/	/	0.9448	/	0.8701	/	/
	MCC	/	/	/	0.8948	/	0.7685	/	/

Table 5: Modalities of Twitter user information that each compared method uses is summarized in this table. The definition of semantic, property and neighborhood user information follows the problem definition in Section 3.

	Lee <i>et al.</i> [16]	Yang <i>et al.</i> [32]	Kudugunta <i>et al.</i> [14]	Wei <i>et al.</i> [29]	Miller <i>et al.</i> [21]	Cresci <i>et al.</i> [5]	Botometer [9]	Alhosseini <i>et al.</i> [1]
Semantic	✓		✓	✓	✓	✓	✓	
Property	✓	✓	✓		✓		✓	✓
Neighbor							✓	✓

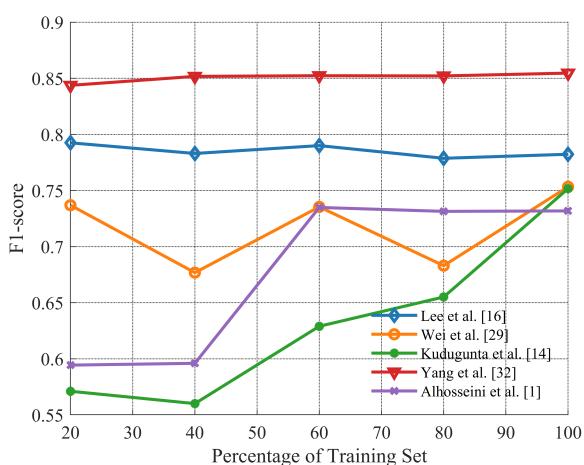


Figure 5: Baseline performance when trained on different percentage of the TwiBot-20 training set. Note that bot detection performance is evaluated on the full test set of TwiBot-20.

Figure 5 demonstrates that even trained on a small portion of our proposed TwiBot-20, competitive baselines like Yang *et al.* [32] still maintain their performance. This indicates that TwiBot-20 can sufficiently train bot detectors, while other datasets with significantly fewer users would not stably benchmark bot detection methods.

6.4 User Information Study

The task of Twitter bot detection is different from the standardized tasks in computer vision and natural language processing in that the input of bot detectors greatly vary from one another. Previous methods rely heavily on either tweet semantics analysis or user profile feature extraction, while methods that stress following behaviour and the graph structure it forms is on the rise. We summarize competitive bot detection baselines and their usage of multi-modal user information in Table 5.

Along with the experiment results in Table 4, we make the following observations:

- To the best of our knowledge, TwiBot-20 is the first publicly available Twitter bot detection dataset to provide follow relationships between users to allow community-based detection measures. By providing multi-modal semantic, property and neighborhood user information, TwiBot-20 successfully supports all baseline bot detectors with varying demand of user information, while previous benchmarks fail to support newer research efforts such as Alhosseini *et al.* [1].
- According to Table 5, Kudugunta *et al.* [14] leverages semantic and property information while Wei *et al.* [29] only uses semantic information. It is demonstrated in Table 4 that Kudugunta *et al.* [14] outperforms Wei *et al.* [29] on our proposed TwiBot-20. A similar contrast could be found between Alhosseini *et al.* [1] and Miller *et al.* [21]. These performance gaps suggest that robust bot detection methods should leverage as much user information as possible.

Therefore, TwiBot-20 would be the ideal dataset to suffice the need for multi-modal user information and fairly evaluate any previous or future bot detectors.

6.5 User Diversity Study

Previous datasets often focus on several specific types of Twitter bots and fall short of comprehensiveness. Another important aim of our proposed TwiBot-20 is to provide a stable benchmark that evaluates bot detectors' ability to identify diversified bots that co-exist on online social media. To prove that achieving good performance on one type of bot doesn't necessarily indicate the ability to identify diversified bots, we train the community-based bot detector Alhosseini *et al.* [1] on only one of the four interest domains in TwiBot-20 and evaluate it on the full test set. We present its performance in Figure 6.

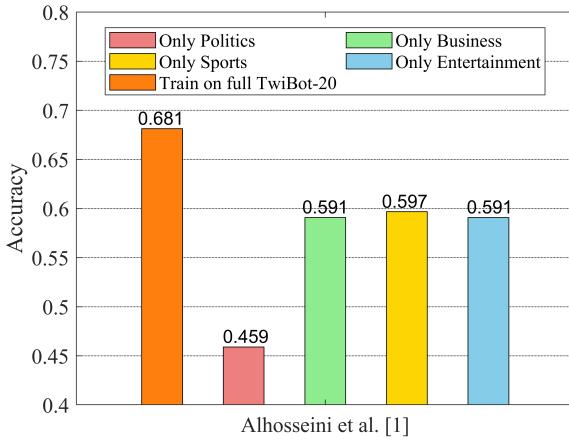


Figure 6: The community-based Alhosseini *et al.* [1]'s performance when trained on one interest domain in comparison to training on the full TwiBot-20. Note that bot detection performance is evaluated on the full test set of TwiBot-20.

Figure 6 illustrates that when the method is trained on one of the user interest domains, Alhosseini *et al.* [1] fails to match its performance when it is trained on the full TwiBot-20. As a result, TwiBot-20 could better evaluate bot detection measures in that it contains diversified bots and genuine users, which demands bot detectors to jointly capture different types of bots rather than being limited to a specific bot detection scenario.

7 CONCLUSION AND FUTURE WORK

Social media bot detection is attracting increasing research interests in recent years. We collected and annotated Twitter data to present a comprehensive Twitter bot detection benchmark TwiBot-20, which is representative of the diversified Twittersphere and captures different types of bots that co-exist on major social media platforms. We make TwiBot-20 public, hoping that it would alleviate the lack of comprehensive datasets in Twitter bot detection and facilitate further research. Extensive experiments demonstrate that state-of-the-art bot detectors fail to match their previously reported

performance on TwiBot-20, which shows that Twitter bot detection is still a challenging task and demands continual efforts. In the future, we plan to study novel Twitter bots and propose robust bot detectors.

REFERENCES

- [1] Seyed Ali Alhosseini, Raad Bin Tareaf, Pejman Najafi, and Christoph Meinel. 2019. Detect Me If You Can: Spam Bot Detection Using Inductive Representation Learning. In *Companion Proceedings of The 2019 World Wide Web Conference*. 148–153.
- [2] Jonathon M Berger and Jonathon Morgan. 2015. The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter. *The Brookings project on US relations with the Islamic world* 3, 20 (2015), 4–1.
- [3] Zi Chu, Steven Gianvecchio, Haining Wang, and Sushil Jajodia. 2012. Detecting automation of twitter accounts: Are you a human, bot, or cyborg? *IEEE Transactions on Dependable and Secure Computing* 9, 6 (2012), 811–824.
- [4] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi. 2015. Fame for sale: Efficient detection of fake Twitter followers. *Decision Support Systems* 80 (2015), 56–71.
- [5] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi. 2016. DNA-inspired online behavioral modeling and its application to spambot detection. *IEEE Intelligent Systems* 31, 5 (2016), 58–64.
- [6] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, and Maurizio Tesconi. 2017. The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. In *Proceedings of the 26th international conference on world wide web companion*. 963–972.
- [7] S. Cresci, F. Lillo, D. Regoli, S. Tardelli, and M. Tesconi. 2018. \$FAKE: Evidence of Spam and Bot Activity in Stock Microblogs on Twitter. In *ICWSM*.
- [8] Stefano Cresci, Marinella Petrocchi, Angelo Spognardi, and Stefano Tognazzi. 2018. From reaction to proaction: Unexplored ways to the detection of evolving spambots. In *Companion Proceedings of the The Web Conference 2018*. 1469–1470.
- [9] Clayton Allen Davis, Onur Varol, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer. 2016. Botornot: A system to evaluate social bots. In *Proceedings of the 25th international conference companion on world wide web*. 273–274.
- [10] Ashok Deb, Luca Luceri, Adam Badaway, and Emilio Ferrara. 2019. Perils and Challenges of Social Media and Election Manipulation Analysis: The 2018 US Midterms. In *Companion Proceedings of The 2019 World Wide Web Conference* (San Francisco, USA) (WWW '19). Association for Computing Machinery, New York, NY, USA, 237–247. <https://doi.org/10.1145/3308560.3316486>
- [11] Emilio Ferrara. 2017. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. *CoRR* abs/1707.00086 (2017). arXiv:1707.00086 <http://arxiv.org/abs/1707.00086>
- [12] Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia, and Alok N Choudhary. 2012. Towards online spam filtering in social networks.. In *NDSS*, Vol. 12. 1–16.
- [13] Zafar Gilani, Reza Farahbakhsh, Gareth Tyson, Liang Wang, and Jon Crowcroft. 2017. Of bots and humans (on twitter). In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* 2017. 349–354.
- [14] Sneha Kudugunta and Emilio Ferrara. 2018. Deep neural networks for bot detection. *Information Sciences* 467 (2018), 312–322.
- [15] Kyumin Lee, Brian Eoff, and James Caverlee. 2011. Seven months with the devils: A long-term study of content polluters on twitter. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 5.
- [16] Kyumin Lee, Brian Eoff, and James Caverlee. 2011. Seven months with the devils: A long-term study of content polluters on twitter. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 5.
- [17] Sangho Lee and Jong Kim. 2013. Warningbird: A near real-time detection system for suspicious urls in twitter stream. *IEEE transactions on dependable and secure computing* 10, 3 (2013), 183–195.
- [18] Brian W Matthews. 1975. Comparison of the predicted and observed secondary structure of T4 phage lysozyme. *Biochimica et Biophysica Acta (BBA)-Protein Structure* 405, 2 (1975), 442–451.
- [19] Michele Mazza, Stefano Cresci, Marco Avvenuti, Walter Quattrociocchi, and Maurizio Tesconi. 2019. Rtbust: Exploiting temporal patterns for botnet detection on twitter. In *Proceedings of the 10th ACM Conference on Web Science*. 183–192.
- [20] Michele Mazza, Stefano Cresci, Marco Avvenuti, Walter Quattrociocchi, and Maurizio Tesconi. 2019. Rtbust: Exploiting temporal patterns for botnet detection on twitter. In *Proceedings of the 10th ACM Conference on Web Science*. 183–192.
- [21] Zachary Miller, Brian Dickinson, William Deitrick, Wei Hu, and Alex Hai Wang. 2014. Twitter spammer detection using data stream clustering. *Information Sciences* 260 (2014), 64–73.
- [22] Amanda Minnich, Nikan Chavoshi, Danai Koutra, and Abdullah Mueen. 2017. BotWalk: Efficient adaptive exploration of Twitter bot networks. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* 2017. 467–474.

- [23] Rizal Setya Perdana, Tri Hadiah Muliawati, and Reddy Alexandro. 2015. Bot spammer detection in Twitter using tweet similarity and time interval entropy. *Jurnal Ilmu Komputer dan Informasi* 8, 1 (2015), 19–25.
- [24] Mohsen Sayyadiharikandeh, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. 2020. Detection of novel social bots by ensembles of specialized classifiers. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*. 2725–2732.
- [25] Gray Stanton and Athirai A Irissappane. 2019. GANs for semi-supervised opinion spam detection. *arXiv preprint arXiv:1903.08289* (2019).
- [26] Kurt Thomas, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song. 2011. Design and evaluation of a real-time url spam filtering service. In *2011 IEEE symposium on security and privacy*. IEEE, 447–462.
- [27] Onur Varol, Emilio Ferrara, Clayton Davis, Filippo Menczer, and Alessandro Flammini. 2017. Online human-bot interactions: Detection, estimation, and characterization. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 11.
- [28] Onur Varol, Emilio Ferrara, Clayton Davis, Filippo Menczer, and Alessandro Flammini. 2017. Online human-bot interactions: Detection, estimation, and characterization. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 11.
- [29] Feng Wei and Uyen Trang Nguyen. 2019. Twitter Bot Detection Using Bidirectional Long Short-term Memory Neural Networks and Word Embeddings. In *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 101–109.
- [30] Chao Yang, Robert Harkreader, and Guofei Gu. 2013. Empirical evaluation and new design for fighting evolving twitter spammers. *IEEE Transactions on Information Forensics and Security* 8, 8 (2013), 1280–1293.
- [31] Kai-Cheng Yang, Onur Varol, Clayton A Davis, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer. 2019. Arming the public with artificial intelligence to counter social bots. *Human Behavior and Emerging Technologies* 1, 1 (2019), 48–61.
- [32] Kai-Cheng Yang, Onur Varol, Pik-Mai Hui, and Filippo Menczer. 2020. Scalable and generalizable social bot detection through data selection. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 34. 1096–1103.