International Journal of Technology and Human Interaction
Volume 19 • Issue 1

Behaviour and Bot Analysis on Online Social Networks:

Twitter, Parler, and Reddit

Sanaz Adel Alipour, Dalhousie University, Canada*
https://orcid.org/0000-0003-0312-8141

Rita Orji, Dalhousie University, Canada

Nur Zincir-Heywood, Dalhousie University, Canada

ABSTRACT

The internet is home to a multitude of social networks that provide users with a sense of community and connection across the world. Among these, Twitter and Reddit are two of the most popular. While Twitter users follow and interact with other users (tweets), Reddit users follow and interact with communities known as subreddits. In addition to mainstream social networks, alternative platforms such as Parler exist for users who prefer less moderated online environments. However, there are also malicious users, such as bots and trolls, who exploit social networks for malicious purposes. Therefore, separating malicious behaviors from legitimate ones is crucial. This research aims to evaluate Botometer and RepScope systems to analyze the temporal posting behaviors of Twitter, Reddit, and Parler users and to identify bots, trolls, and malicious behaviors.

KEYWORDS

Bot/Human Identification, Online Social Networks, Parler, Reddit, Twitter

INTRODUCTION

By providing virtual environments, online social networks allow humans to communicate and interact with each other in different ways to achieve their business, political, economic, and social goals. Twitter, Parler, and Reddit are well-known online social platforms that have attracted a lot of users based on the characteristics and functionalities they provide. For example, Twitter (https://twitter.com) is one of the most popular social network platforms where users can share and distribute information. Parler (https://parler.com), which is considered an alternative platform to Twitter, attracts users to the less moderated environment and to its filtration system, which allows them to block interactions with others that match their selected filters (Aliapoulios et al., 2021). On the other hand, Reddit (https://

DOI: 10.4018/IJTHI.327789

*Corresponding Author

www.reddit.com) provides a forum-based platform in which users can benefit from the news they are interested in by subscribing to the appropriate subreddits and exchanging comments.

The accuracy of the information shared and of the user's identity is essential for social platforms. Social bots or users with malicious goals can be a threat to the accuracy of information and resources shared on social platforms. This group of users tries to act like legitimate users (for example, following other users, voting on posts created by other users, or engaging in different discussions) so that they can achieve their malicious goals without being detected (Najari et al., 2022). Various approaches have been proposed for identifying bots on social networking platforms, most of which are associated with Twitter. The most popular identification tool on Twitter is Botometer, through which bots and legitimate accounts (human accounts) are classified based on their characteristics such as metadata, content, and timing features. In accordance with the classification done by Latah et al. (2020), Botometer's identification approach can be classified as machine-learning-based. In our previous work (Adel Alipour et al., 2022), we benchmarked Botometer and Tweetbotornot on publicly available labeled Twitter datasets to evaluate their performance. We then went further and proposed two new methods that could be used independently (Method 1, aka RepScope) and as an add-on (Method 2) to Botometer for improving Twitter bot identification. We evaluated the new methods on the same datasets that were used for benchmarking Botometer and Tweetbotornot. We could obtain high accuracy in identifying both bots and humans on Twitter using a much simpler approach than Botometer or Tweetbotornot. However, note that Botometer and Tweetbotornot can work only on Twitter data, whereas RepScope can potentially work on other social networks as well. In a nutshell, RepScope indicates the scope of the repetitive behavior of a user. In this research, we extend RepScope in two ways: (1.) we aim to improve upon RepScope by providing guidelines to choose online networks with appropriate thresholds and (2.) we analyze the generalizability of RepScope on different data from three different social networks; namely, Twitter, Parler, and Reddit. Among social platforms, we chose Twitter and Reddit because of their popularity, and Parler because of its alternative nature, providing fewer restrictions for users in publishing information, which in return could make it more vulnerable compared with other ones. The obtained results show that by considering the same threshold values, RepScope is able to identify malicious and legitimate behaviors on Twitter and Reddit datasets using the same configurations. However, the configuration of RepScope needs to be changed to identify legitimate and malicious users on Parler.

In the following sections of this paper, we present an overview of the related works, introduce our methodology, and share the results and evaluations. Finally, we discuss our conclusions and recommendations for future work.

LITERATURE REVIEW

In this section, we provide a summary of recent research done to identify different behaviors and bots on online social networks. Latah (2020) proposed approaches for identifying social bots that can be categorized into three main approaches: graph-based approaches, machine-learning approaches, and emerging ones. Graph-based approaches detect bots by examining the connections and relationships in social graphs. Machine learning approaches include supervised learning in which a set of features are used to interpret the behavior of human or bot accounts, unsupervised learning in which frequent patterns are determined without relying on labeled data, and hybrid learning, which combines supervised and unsupervised learning. Emerging approaches, such as natural language processing, were introduced to improve the social bot detection approaches.

In the context of social bot identification, several studies have focused on Twitter, but Reddit, and specifically Parler, have received less attention. Martin-Gutierrez et al. (2021) introduced an approach for detecting bots on Twitter that leverages advanced deep-learning techniques and multilingual language models. Their method involved generating encodings of text-based features from user accounts using state-of-the-art models that were then combined with metadata and processed using a dense neural network architecture called Bot-DenseNet. Najari et al. (2022) used Generative Adversarial Network (GAN) and proposed a new framework for detecting bots on Twitter by extracting the behavioral pattern from data. Gera and Sinha (2022) proposed a machine-learning-based, AI-driven bot detection framework for identifying bots on Twitter using basic features. In this research, they analyzed the bots' tweeting behavior and showed that bots on Twitter have high uniformity in the rate of sending tweets. The Centroid Initialization Algorithm (CIA) is a phase of their framework that handles unbalanced datasets (Gera & Sinha, 2022). Hayawi et al. (2022) presented a deep learning-based framework for classifying bots versus human accounts on Twitter; their work focused on profile metadata features (including text features as well as numerical and binary features). In a different research investigation, Koggalahewa et al. (2022) introduced an unsupervised spammer detection technique; their content-based approach relies on users' peer acceptance, determined through an analysis of shared interests and topics among users. Their method examines the patterns of common interests and topics to differentiate spammers from genuine users on Twitter without the need for manual labeling Koggalahewa et al. (2022).

Costa et al. (2015) proposed a method that can identify both human and bot users on Twitter and Reddit that consists of different steps, including discovering patterns, modeling the patterns, and using the model for detecting bots. In this study, they relied on temporal activities by users (Costa et al., 2015). Hurtado et al. (2019) presented an approach for identifying bots on the Reddit social network that concentrates on the comments left by users and proposed a network-based approach. In this research, they identified abnormal users by creating two networks—post-to-post and user-to-user—and analyzing the number of users who commented on more than one post in a specific subreddit and the interval time between the comments left by them. In another study, Ashford et al. (2020) specifically targeted Reddit to gain insight into and identify disruptive behavior without relying on content analysis. By analyzing user activity, such as reply patterns and temporal statistics, they showed that it was possible to accurately predict signs of disruptive behavior. Their finding demonstrated the effectiveness of using limited inputs to detect disruptive behavior (Ashford et al., 2020). Saeed et al. (2021) proposed a system (TROLLMAGNIFIER) for identifying troll accounts on Reddit; they used ground-truth troll accounts and extracted those accounts having interaction with these troll accounts among the data collected through the Pushshift Reddit application programming interface (API) (Baumgartner et al., 2020). By having these two datasets (as negative and positive classes), Saeed et al. (2021) then trained a model for identifying troll accounts in the wild. By using content-agnostic features (e.g., total comments, total submissions, and account age) and Random Forest as a classifier, they could achieve the best results compared with the other classifiers they used (Saeed et al., 2021).

In other research, Urbaniak et al. (2022) extracted the relationships between the usernames and users' behavior on Reddit and analyzed the relationships; they found that toxic usernames (those containing toxic words) tend to create more toxic content (posts and comments) and are more likely to be suspended. Ravazzi et al. (2022) suggested that malicious accounts from fringe social networks such as Parler penetrate the mainstream social networks such as Twitter after becoming popular. Therefore, it is crucial to identify them before they affect mainstream social networks. Ravazzi et al. (2022) also stated that addressing such a problem on fringe social networks is complicated because of the nature of these networks (lack of adequate information). In this research, they proposed a method for detecting bots by modeling the agents and opinions they left on different topics, and then they examined the identified bots' impact on mainstream social networks Ravazzi et al. (2022).

In summary, the focus of recent research has been on extracting and engineering effective features to identify different behaviors, including bots/humans, on online social networks as accurately as possible. In our research, we concentrate on analyzing different behaviors, such as Trolls, bots and humans, on data from different online social networks, including mainstream and fringe ones, to explore and understand the effectiveness and generalizability of the existing and proposed systems in identifying malicious and legitimate users.

METHODOLOGY

In our previous work (Adel Alipour et al., 2022), we reproduced and evaluated the state-of-the-art systems—namely, Botometer and Tweetbotornot—on several publicly available datasets employed in the literature for Twitter bot analysis. Based on the results obtained, Botometer was more successful than Tweetbotornot on the majority of the datasets (Adel Alipour et al., 2022). Moreover, we showed that our proposed method, RepScope, could detect an outstanding number of bot and human accounts on Twitter correctly and could be used as an add-on system to improve Botometer results accuracy as well.

To effectively use both Botometer and RepScope, we established threshold values to distinguish between bot and human accounts. Although Botometer thresholds were determined based on previous studies, guidelines for selecting RepScope thresholds were not available. The primary objective of this study is to assess the generalizability of RepScope across various social networks. The features employed by RepScope are not specific to any particular platform because all social networks serve as platforms for users to share information, although the terminology used may vary. For instance, Twitter refers to shared information as tweets, whereas Reddit uses the term submissions. However, note that the selection of thresholds in RepScope may vary depending on the specific social network analyzed. Therefore, understanding the process of choosing appropriate thresholds tailored to each platform is crucial. In this section, we provide an overview of Botometer and RepScope, followed by a guideline for choosing RepScope thresholds. We then evaluate the performance of Botometer and RepScope on a new Twitter dataset consisting of unlabeled data and assess their respective performances. Furthermore, we explore the generalizability of RepScope by applying and evaluating it on diverse datasets from Twitter, Reddit, and Parler. The subsequent subsections introduce the various social media platforms and their corresponding datasets on which RepScope is employed.

Social Media Platforms

Twitter is a microblogging social platform on which users interact with each other through messages known as tweets. According to Dixon (2022), a report on statista.com indicated that the number of monetized daily active users on Twitter has been reported as approximately 238 million. Twitter is a popular social network, particularly in the United States, where according to Dixon (2022), about 77 million people use the service. Statistics presented by Watson (2023) also show that more than half of the users on Twitter use this platform for news.

Parler is another microblogging social platform (Cox, 2020) that has been likened to a "conservative Twitter" because it is a similar platform of which many users are noted Republicans and right-wing voices (Herbert, 2020). The "freedom of speech" and "protecting users' rights" concepts on Parler are assumed to be the compelling reasons why a significant number of users have immigrated from social platforms such as Twitter to Parler to avoid being suspended or blocked (Aliapoulios et al., 2021). Parler users can create posts (similar to tweets on Twitter) and leave comments on other users' posts or comments.

Reddit, on the other hand, is a platform for social news aggregation. Based on 2022 reports in Dixon (2023), there are around 50 million users who are active daily on Reddit. On Reddit, users can subscribe to different communities (subreddits) based on their interests and create submissions (similar to tweets on Twitter). They also can leave comments on the submissions that have been already posted or reply to them.

Botometer and RepScope

Botometer is a supervised machine learning classifier for identifying social bots on Twitter, which has attracted a lot of attention. Botometer extracts more than 1,000 features from each Twitter account to score it as bot versus human. These features are employed in the user metadata, friends, content, sentiment, network, and timing (Varol et al., 2017). In summary, it works by receiving the screen name or user ID of a user as input and by examining the account, using more than value features for calculating a score as an output. These Botometer scores range from 0 to 5 (or a normalized range from 0 to 1) and indicate whether the account is more likely to be a bot or human. To use this tool, a threshold value must be established to determine whether an account is a bot or a human based on the threshold. Taking the threshold value of 0.5 (for the range 0 to 1) as an example, accounts with a Botometer score of more than or equal to 0.5 are designated as bots, whereas those with a score of less than 0.5 are designated as humans.

RepScope, shown in Figure 1, was inspired by the approach used by Martini, et al. (2021). Their method evaluated accounts based on the number of tweets (those tweets that contain certain hashtags) they sent per day and separated as bot or human. Their focus was on political data. We were inspired by their approach as well as the feature adopted by Botometer, which was categorized as the Timing feature. Timing refers to the time between two consecutive days (Varol et al., 2017). Using this feature and the repetitive behavior heuristic algorithm, we analyzed how bots and humans behave based on the frequency of tweeting and the repetition of their behavior over time. To this end, we designed and developed RepScope (Adel Alipour et al., 2022), where we extracted the date of the tweets sent by each account and calculated the number of bot and human accounts identified based on different values of two thresholds (Threshold-1 and Threshold-2). Threshold-1 refers to the number of consecutive days a user tweets every single day, whereas Threshold-2 refers to the number of different consecutive days in which a user tweets at least one tweet on each day of those consecutive days. By considering Threshold-2 as the threshold, if an account sends tweets over two or more consecutive days and repeats its behavior less frequently than a given threshold value, it is categorized as being a bot, whereas the accounts that do not are categorized as being humans.

As discussed in Varol et al. (2017), more than 1,000 features are used in Botometer to identify whether a user is a bot or a human. These features are classified into six classes: metadata, friends, content, sentiment, network, and timing. For examining the effectiveness of the features, models have been trained by each of those among which metadata and content have shown the best results (Varol et al., 2017). The results given by RepScope showed that consecutive days of sending tweets can be considered a feature that strongly affects identifying different behaviors.

Choosing Values for RepScope Thresholds

Regarding Threshold-1, we obtain the consecutive days in which each account sent tweets (on each day of those consecutive days) and sorted them from minimum to maximum. Then, for each of these obtained consecutive days, we calculated how many accounts, the maximum number of consecutive days in which they have sent tweets, are equal to each of the obtained consecutive days. We did this for all datasets in our previous work (Adel Alipour et al., 2022) and tried to find the best point through which the maximum number of bots and human accounts were identified in all datasets (both datasets consisting of human accounts and those consisting of bots). Threshold-2 values were chosen in the same manner.

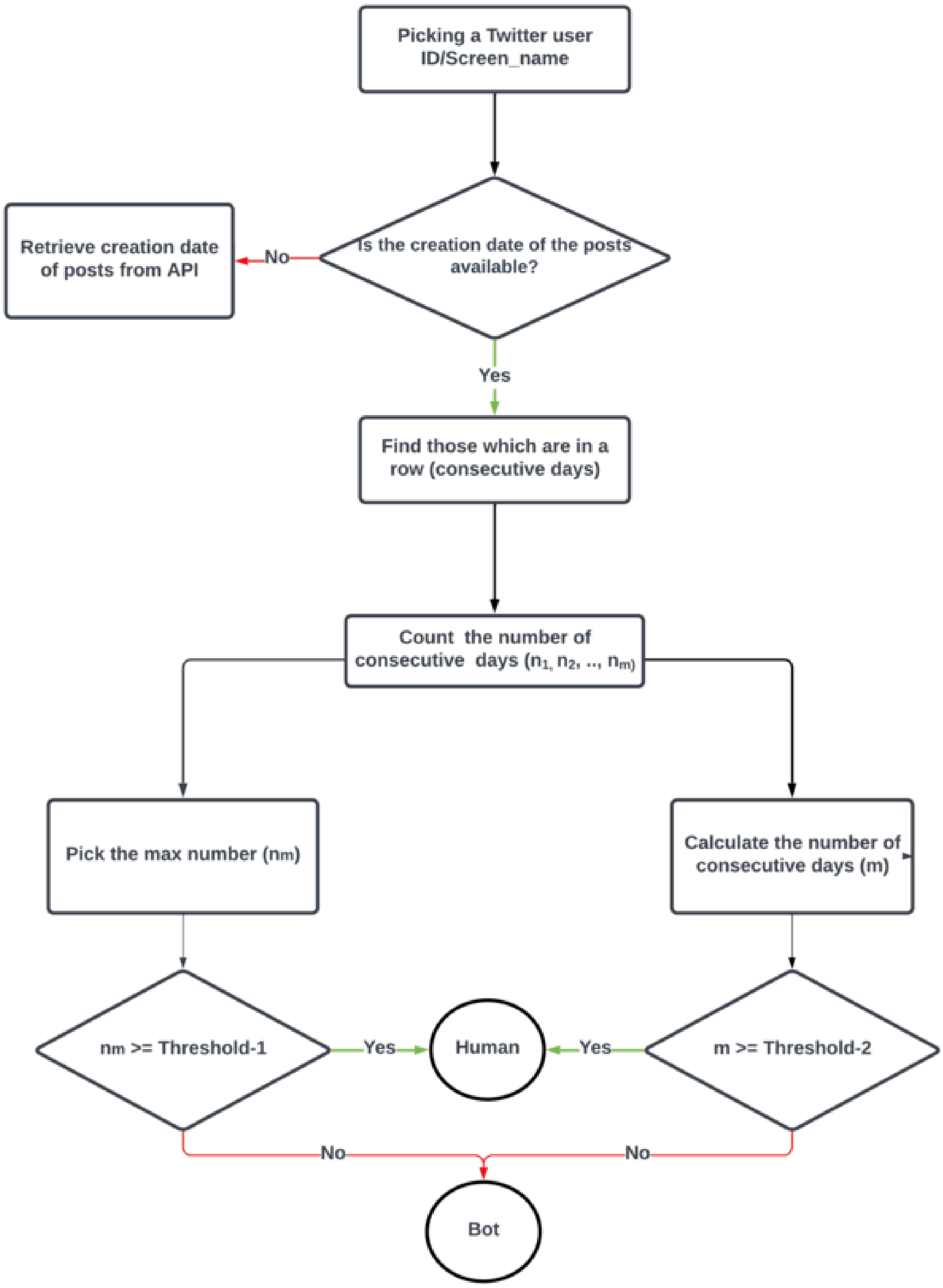
Datasets

In this research, we used naturally different publicly available datasets corresponding to three different social platforms, including Twitter, Reddit, and Parler. In the following sections, we provide more details about the datasets used in this study, including information about their availability, collection, size, and labeling.

Availability

In this work, we exclusively used publicly available datasets, which significantly enhances the reproducibility and validation of our study. By relying on publicly accessible datasets, other

Figure 1. RepScope overview


Picking a Twitter user ID/Screen_name
Is the creation date of the posts available?
No
Retrieve creation date of posts from API
Yes
Find those which are in a row (consecutive days)
Count the number of consecutive days (n1, n2, .., nm)
Pick the max number (nm)
Calculate the number of consecutive days (m)
nm >= Threshold-1
Yes
Human
Yes
m >= Threshold-2
No
No
Bot

researchers and practitioners can easily access the same data sources, allowing them to replicate our experiments and verify our findings. This transparency and accessibility of the datasets contribute to the scientific integrity and reliability of our research, promoting a more collaborative and open research environment.

The Twitter datasets we used in our previous research (Adel Alipour et al., 2022) include two subsets: those on which Botometer has been trained, which are publicly available on the Botometer repository (https://botometer.osome.iu.edu/bot-repository/datasets.html), such as Cresci-rtbust-2019; and those on which Botometer has not been trained, such as the ones in Echeverrï£¡a et al. (2018). In this study, we used a new public dataset from Brena et al. (2019), consisting of user IDs that disseminated news articles from major U.S. news outlets on Twitter. We employed Botometer and RepScope on two samples of these user IDs. We refer to these sampled datasets as News-Twitter-Sample1 and News-Twitter-Sample2.

Another dataset used in this research pertains to Reddit users. Saeed et al. (2021) employed it for identifying trolls on the Reddit platform. Trolls are accounts that try to engage other accounts in discussions in a negative way by sharing information that is not true. Saeed et al. (2021) used these publicly available data (known troll accounts) that were released by Reddit as ground truth to train machine learning models. The dataset, publicly available, included usernames of known troll accounts provided by Reddit (Spez, n.d.). The last dataset used in this research is related to the Parler social platform. In our previous research, (Aliapoulios et al., 2021) we provided a public dataset comprising metadata of Parler users and their posts. We used a sample of that data, including Parler users and the creation date of their posts. Hereafter, we refer to this dataset as the Parler Sample dataset. One of the features corresponding to the Parler users in the large Parler dataset is the “Human” feature. In this research, we consider those data records with “Human=True” as humans and those with “Human=False” as bots.

Data Collection

To apply our method to these datasets, we required the creation dates of recent posts made by each user, specifically tweets on Twitter and submissions on Reddit. The Parler dataset already included the posts and their creation dates, but for Twitter and Reddit, we collected the necessary data by using the Twitter API (https://developer.twitter.com/en/docs/twitter-api) and the Python Reddit API Wrapper (PRAW: The Python Reddit API Wrapper — PRAW 7.6.2.dev0 documentation), resulting in the creation of the dataset known as Reddit-Known-Trolls.

To use the Twitter API and Reddit API, we first created a Twitter/Reddit Developer Account, which provided us with the necessary API credentials. With these credentials in hand, we could make requests to the desired API endpoints and were then able to access and use the Twitter/Reddit API’s functionalities effectively.

Dataset Size and Labeling

In our previous work, we successfully applied our method to datasets on which Botometer was trained, as well as other labeled datasets (Adel Alipour et al., 2022). Building upon these results, for this study, we extended our research by incorporating an additional publicly available Twitter dataset without labels. Furthermore, we explored the applicability of our method across different social networks, such as Reddit and Parler. Table 1 summarizes the datasets employed in this research.

Table 1. The datasets correspond to the three different social platforms: Twitter, Reddit, and Parler (size in the number of records)

Dataset	Size	Type
News-Twitter-Sample1	451	Unlabeled
News-Twitter-Sample2	323	Unlabeled
Reddit-Known-Trolls	938	Labeled as bots
Parler-Sample	558	Labeled as bots (528) and humans (30)

RepScope Limitations

As previously mentioned, we used publicly available datasets for our research, with the Parler dataset providing comprehensive data. However, for Twitter and Reddit datasets, we relied on retrieving the creation dates of user posts, which depends on the platforms' availability. Note that Parler has recently been shut down by its new owner, making it impossible to retrieve data for new users, unless the platform resumes operation. This limitation affects not only our method but also other feature extraction-based approaches that rely on data retrieval.

Another limitation arises from the restrictions imposed by the APIs (of Twitter and Reddit). These platforms have limitations on the number of data that can be retrieved within a specific time frame. Thus, we are restricted in terms of the amount of data we can retrieve for analysis. Such limitations can impact the scope of the analysis relying on these APIs, including ours, because we may not be able to access the complete set of data.

RESULTS AND DISCUSSION

In this section, we first summarize the results of our previous paper, those related to applying RepScope on 15 different Twitter datasets (Adel Alipour et al., 2022). We examined the results of software over the air (SOTA) systems, including Botometer and Tweetbotornot, but for the purpose of analyzing the proposed new method (RepScope), we considered only Botometer results because in contrast to Botometer researchers (Botometer repository reference), Tweetbotornot researchers did not provide details about which datasets Tweetbotornot was trained on. Therefore, our analysis focused on Botometer and summarized the results from our previous research (Adel Alipour et al., 2022) corresponding to the 15 labeled datasets. We then analyzed RepScope performance on a new Twitter dataset. Apart from the Twitter datasets, we were also taking a step further and using non-Twitter datasets, which are Reddit and Parler, including data corresponding to Reddit and Parler social platforms. This step was important for evaluating the generalizability of RepScope against different social networks (such as Parler and Reddit) as well as against the performance of the state-of-the-art system, Botometer. Note that in Twitter datasets, dataset size refers to the number of accounts Botometer has identified as bot or human. Many accounts fall into the categories of "not found," "forbidden," and "unauthorized," reflecting that these accounts have already been suspended or deleted by Twitter.

RepScope on Labeled Twitter Datasets

Regarding the performance, the common bot and human accounts to both Botometer and RepScope were examined. Tables 2 and 3 summarize the results obtained by RepScope and Botometer on the labeled datasets. As Table 2 shows, in all datasets except Kaiser and Botwiki, more than half of the accounts were correctly identified as bots (true positives, or TPs) using RepScope. Also, in most datasets, the number of commonly identified bots and the number of bots identified by Botometer showed that RepScope was able to detect most of the bots Botometer was able to detect. Another important factor was that common bots constituted the majority of the bots identified by each method in most datasets.

Table 3 reveals that using Threshold-2, RepScope was able to identify more accounts as bots compared with Threshold-1 (Table 2). In general, the number of TPs is greater than the number of FNs (false negatives or bot accounts that were identified as human). By comparing the number of common bots and the number of bots identified by Botometer, we discovered that RepScope (when Threshold-2 is chosen) correctly identifies most of the bots (including bots available in Kaiser and Botwiki-2019) detected by Botometer. Also, in some datasets, including TwiBot-20, Cresci-rtbust-2019, Astroturf, Journalist attack bots (Brian), and DeBot, RepScope has been more successful than Botometer.

Table 2. The number of bots identified correctly by RepScope (by considering 6 as the threshold-1 value), correctly identified bots by Botometer (by considering 0.5 as the value of threshold), and the number of common bots in Twitter datasets containing accounts labeled as bots

Dataset	Size	Identified Bots		
		Common	RepScope	Botometer
Cresci	303	230	256	243
BotoFeed	90	46	52	74
Kaiser	1,503	352	465	1,306
Vendor	685	443	506	546
Pronbots	1,616	1,278	1,389	1,453
Astroturf	171	96	128	127
Political	13	13	13	13
Botwiki	649	58	58	649
TwiBot-20	4,060	859	2,476	1,228
BurstyUsers	1,967	1,967	1,967	1,967
Ben Nimmo	826	338	528	556
Brian	637	526	598	543
DeBot	749	216	501	264

Note: Cresci-rtbust-2019, Botometer-feedback-2019, Kaiser, Vendor-purchased-2019, Pronbots-2019, Astroturf, Political-bots-2019, Botwiki-2019, TwiBot-20, Journalist attack bots (Ben Nimmo), Journalist attack bots (Brian), and DeBot are the full names of the datasets.

Table 3. Number of bots identified correctly by RepScope (by considering 6 as threshold-2 value), correctly identified bots by Botometer (by considering 0.5 as the value of threshold), and the number of common bots in Twitter datasets containing accounts labeled as bot

Dataset	Size	Identified Bots		
		Common	RepScope	Botometer
Cresci	303	228	275	243
BotoFeed	90	57	67	74
Kaiser	1,503	1,005	1,082	1,306
Vendor	685	480	486	546
Pronbots	1,616	1,322	1,373	1,453
Astroturf	171	119	159	127
Political	13	13	13	13
Botwiki	649	589	590	649
TwiBot-20	4,060	871	2,111	1,228
BurstyUsers	1,967	1,967	1,967	1,967
Ben Nimmo	826	505	619	556
Brian	637	521	560	543
DeBot	749	234	569	264

Note: Cresci-rtbust-2019, Botometer-feedback-2019, Kaiser, Vendor-purchased-2019, Pronbots-2019, Astroturf, Political-bots-2019, Botwiki-2019, TwiBot-20, Journalist attack bots (Ben Nimmo), Journalist attack bots (Brian), and DeBot are the full names of the datasets.

Regarding datasets in which accounts are labeled as human, our analysis showed that RepScope (by considering Threshold-1 or Threshold-2) was also successful in identifying more than half of human accounts in most datasets where human accounts are labeled. In other words, the number of human accounts identified correctly as human (true negatives, or TNs) outweighs the number of human accounts identified as bot (false positives, or FPs). Results also showed that RepScope was more effective at identifying human accounts when the thresholds were set for the number of repetitions of sending tweets in n-consecutive days (Threshold-2).

In summary, these results show that the number of TPs in datasets including only bot accounts is higher than the number of FNs. Similarly, datasets with human accounts have more TNs than FPs. Using these results and those obtained from Botometer and RepScope, we found that it is obvious that repetition of the behavior of sending tweets over a number of consecutive days seems to be a simple, but key factor in differentiating human versus bot accounts on Twitter.

Threshold Value Selection for RepScope

We plotted the number of accounts into bar charts and assigned them to the corresponding number of consecutive days for each dataset. We then tried to determine Threshold-1 to identify the maximum number of bots and human accounts. Figures 2 and 3 show the bar charts for human (the green ones) and bot datasets (the blue ones), respectively. In these graphs, the y-axis shows the number of accounts, and the x-axis shows the number of consecutive days. For example, Figure 2 (a) shows that, in 250 of the accounts, the maximum number of consecutive days in which they sent tweets each day is 5. Among the human datasets in Figure 2, it seemed that the sum of the number of accounts associated with consecutive days greater than 5 (the bar charts to the right of 5) is greater than the sum of the number of accounts associated with consecutive days less than 5 (the bar charts to the left of 5). This data enabled us to calculate the values that have been shown as pairs placed next to each dataset's name in the caption of Figure 2. These pairs (before 5, after 5) indicate that the number of human accounts that have sent tweets for 5 days or more is more than those that have sent tweets for a maximum of 4 days in a row.

On the other hand, if we consider the same 5 consecutive days in bot datasets (Figure 3), then it seems that the sum of the bar charts on the left side of 5 is more than the sum of the bar charts on the right side of it. This finding indicates that bots tend to tweet less than 5 days in a row. Therefore, according to these observations, the threshold values of consecutive days were considered as 5, 6, and 7. For the second threshold of RepScope (repetitions of sending tweets over consecutive days), we also plotted the same bar charts. This time we studied the results to identify a point on the charts where there is a clear difference between the account totals before and after. Therefore, we again calculated the number of accounts for bot and human datasets. As pairs in the caption of Figures 4 and 5 show, by considering 5 as a threshold (number of repetitions), the sum of the bar charts on the left side of 5 is more than the sum of the bar charts on the right side of it in all bot datasets except TwiBot-20, and vice versa for human datasets except for Cresci-rtbust-2019.

Unlabeled Twitter Dataset, Botometer, and RepScope

Because News-Twitter-Sample1 and News-Twitter-Sample2 are not labeled datasets (we do not know which of them are human accounts and which of them are bot accounts) and RepScope has been already analyzed compared with Botometer results, in our research for this paper, we applied Botometer on these new datasets. This experiment enabled us to understand the performance of Botometer for the identification of bot and human accounts separately. We then applied RepScope to each category. The threshold values are the same as the ones described in the previous section. There are 451 accounts in the News-Twitter-Sample1, of which Botometer identified 108 as bots (using 0.5 as the threshold). As illustrated in Figure 6, RepScope was successful in identifying bots that account for more than 50% of bots detected by Botometer. The percentage rose to 77% when Threshold-2 was chosen. In identifying human accounts, RepScope (when Threshold-1 was chosen) was also able

Figure 2. Related bar graphs to human datasets showing the number of consecutive days and number of accounts that have sent tweets over maximum of these consecutive days. The graphs refer to (a) 'Verified-2019' (397, 1,296), (b) 'TwiBot-20' (1,117, 1,827), (c) 'Kaiser' (774, 1,108), (d) 'Cresci-rtbust-2019' (108, 103), (e) 'Celebrity2019' (1,709, 3,141), and (f) 'Botometer-feedback-2019' (124, 143)

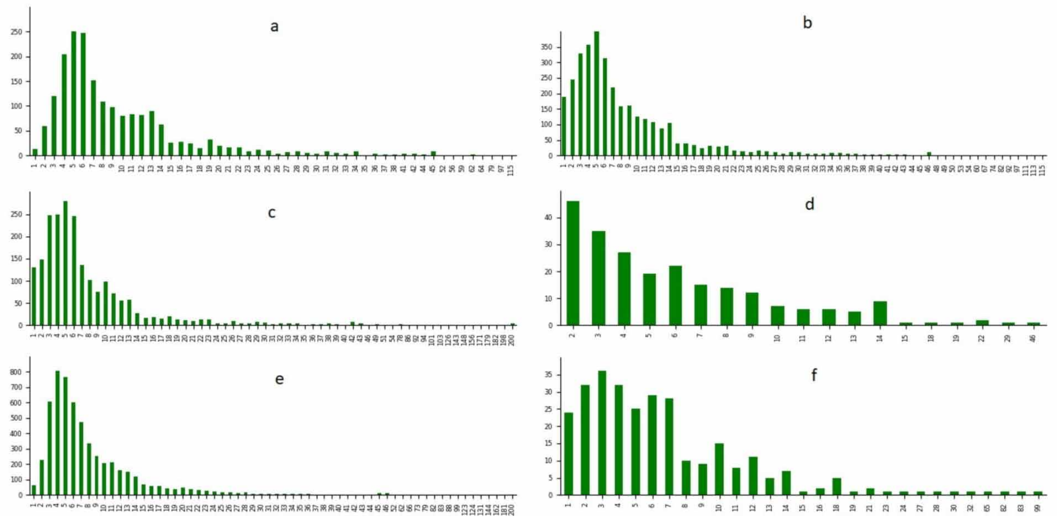
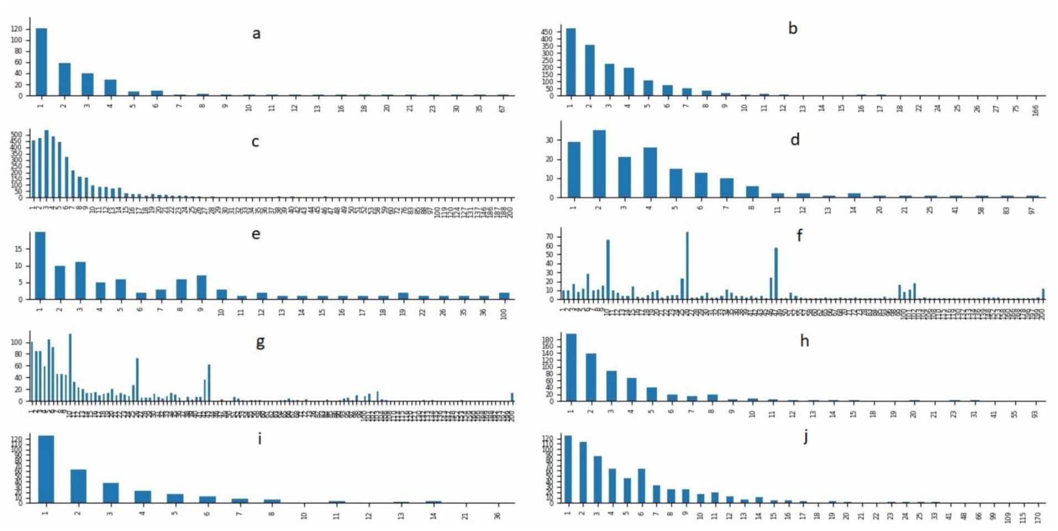


Figure 3. Related bar graphs to bot datasets showing the number of consecutive days and number of accounts that have sent tweets over maximum of these consecutive days. The graphs refer to (a) 'Cresci-rtbust-2019' (128, 28), (b) 'Pronbots-2019' (779, 218), (c) 'Twibot-20' (1,956, 1,594), (d) 'Astroturf' (111, 43), (e) 'Botometer-feedback-2019' (26, 38), (f) 'Botwiki-2019' (45, 589), (g) 'Kaiser' (328, 1,037), (h) 'Journalist Attack Bots (Ben Nimmo)' (295, 96), (i) 'Journalist Attack Bots (Brian)' (122, 39), and (j) 'Debot' (264, 248)



to identify more than 60% of those identified by Botometer (Figure 7). By choosing Threshold-2 as RepScope's threshold, the number of identified human accounts was 171, which constituted 50% of those identified by Botometer. Note that this dataset is not labeled. In our previous research (Adel Alipour et al., 2022), we demonstrated that Botometer scores are more reliable for bot accounts than for human accounts because those associated to human accounts are more likely to be changed in some way to be identified as bots. This led us to collect again the Botometer scores for those human accounts that RepScope (with Threshold-2) did identify as bots (which constituted 172 of the 343

Figure 4. Related bar graphs to bot datasets showing the number of repetitions of sending tweets in n-consecutive days, as well as the related number of accounts. The graphs refer to (a) 'Crescirtbust-2019' (125, 27), (b) 'Pronbots-2019' (816, 235), (c) 'Twibot-20' (1,434, 1,939), (d) 'Astroturf' (124, 12), (e) 'Botometer-feedback2019' (42,22), (f) 'Botwiki-2019' (567, 58), (g) 'Kaiser' (904, 422), (h) 'Journalist Attack Bots (Ben Nimmo)' (210, 203), (i) 'Journalist Attack Bots (Brian)' (93, 74), and (j) 'Debot'(346, 178)

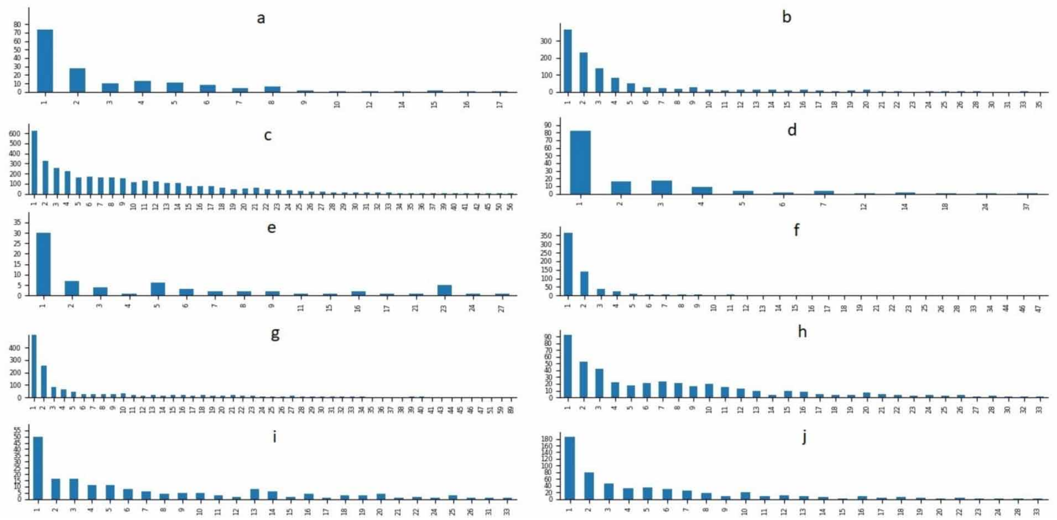
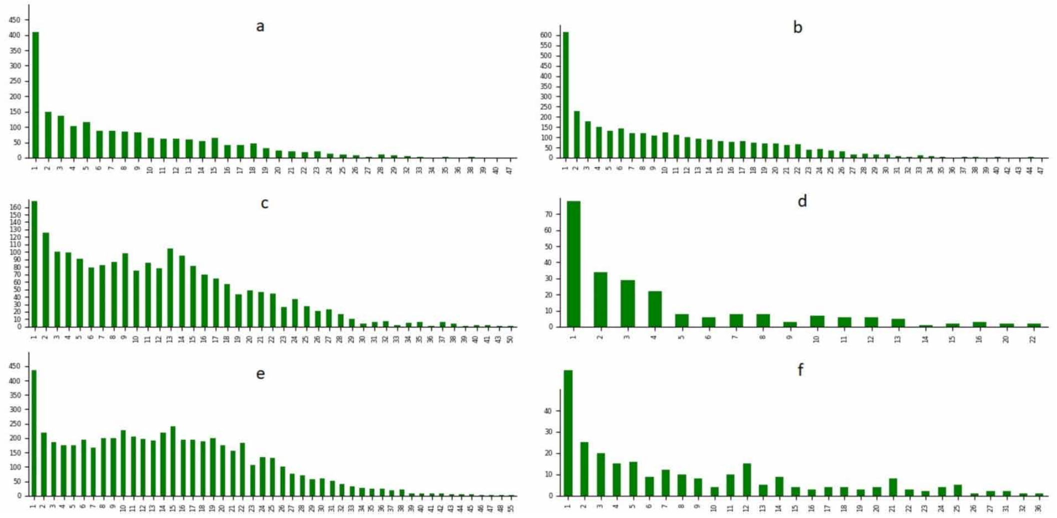


Figure 5. Related bar graphs to human datasets showing the number of repetitions of sending tweets in n-consecutive days, as well as the related number of accounts. The graphs refer to (a) 'Verified-2019' (797, 1,018), (b) 'TwiBot-20' (1,176,, 1846), (c) 'Kaiser' (493, 1,447), (d) 'Cresci-rtbust-2019' (163, 59), (e) 'Celebrity2019' (1,018, 43,54), and (f) 'Botometer-feedback-2019' (119,133)



human accounts identified by Botometer) and identified that 12 accounts classified as bots, which could not be identified by Botometer. These were the main reasons why RepScope and Botometer identified different numbers of bot and human accounts.

We also used another sample dataset (News-Twitter-Sample2) that included 401 accounts, and Botometer identified 78 of them as bots and 323 as human accounts (again by using 0.5 as threshold value). Once again, RepScope was able to identify 74% of bot accounts identified by Botometer as

Figure 6. Number of bot accounts identified by Botometer and RepScope (when Threshold-1 was chosen) in News-Twitter-Sample 1

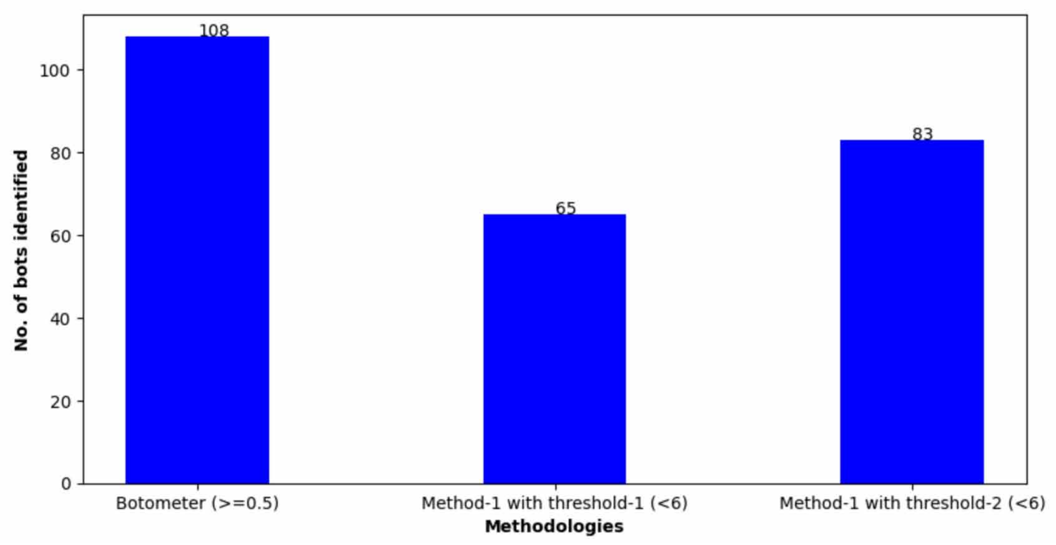
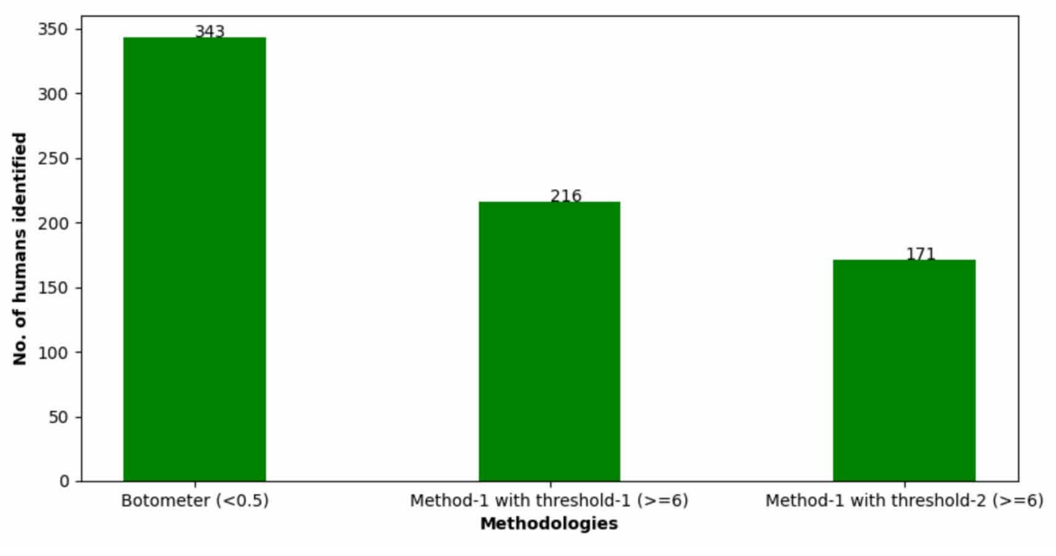


Figure 7. Number of bot accounts identified by Botometer and RepScope (when Threshold-2 was chosen) in News-Twitter-Sample 1



bots. However, the number of human accounts identified by RepScope constituted 41% of those identified by Botometer. After a couple of days, we again obtained the Botometer scores for those human accounts (identified by Botometer) that were identified as bots by RepScope (191 out of 323 human accounts). The new results of applying Botometer showed that 33% of these accounts (64 out of 191) could not be scored (they were identified as Not Found, No Timeline, Forbidden, and Unauthorized), indicating that these accounts have been blocked by Twitter or removed by individuals. Also, 18 of 191 accounts were identified as bots (the new Botometer scores were greater than 0.5). These results show that RepScope is also more successful at identifying human accounts (especially when Threshold-2, repetition of n-consecutive days, is chosen).

Reddit Dataset and RepScope

Given the objectives of Trolls, they could be considered bots on Reddit. However, to the best of our knowledge no publicly available tool to identify Trolls exists. To this end, neither Botometer nor Tweetbotornot tools can be used on Reddit because they employ features specific to Twitter. But the proposed approach, RepScope, is independent from Twitter-specific features, so we employed and evaluated it on different types of social networks, including Reddit. This time instead of tweets on Twitter, we applied the proposed method to the submissions posted by the troll accounts. As shown in Tables 4 and 5, the majority of the troll accounts were reluctant to post submissions on consecutive days and repeat this behavior over time.

Parler Dataset and RepScope

Table 6 shows that by applying RepScope on the posts created by Parler users, the number of nonhuman accounts (whose human feature is false) that created posts on consecutive days is rare compared with

Table 4. Number of consecutive days and the number of accounts posted submissions in maximum these consecutive days on the Reddit-Known-Trolls dataset

No. Cons Days	No. Accounts
0	805
2	92
3	24
4	6
5	9
6	1
10	1

Table 5. Number of repetitions of n-consecutive days and the number of accounts posted submissions on these n-consecutive days on the Reddit-Known-Trolls dataset

Number of	
N-Cons Rep.	Accounts
0	854
2	31
3	21
4	8
5	6
6	3
7	3
8	2
9	3
10	3
11	3
14	1

Table 6. Number of consecutive days and the number of accounts (accounts whose human feature is false and those with human feature of true) that created posts in maximum these consecutive days on the Parler dataset

	Number of	
Con days	Accounts	True "Human" Accounts
0	428	9
2	57	7
3	21	2
4	17	4
5	8	2
6	4	0
7	5	1
8	4	2
9	2	2
10	1	0
11	2	0
12	2	1
15	1	0
16	1	0
17	2	0
22	2	0
31	1	0

those that did not create any posts on consecutive days. Moreover, the number of human accounts (those with the human feature true) that sent posts on consecutive days exceeds the number of those who did not.

In the case of the repetition of sending posts on n-consecutive days, we achieved a similar result (Table 7). Therefore, we concluded that by choosing 2 as the value of both thresholds (Threshold-1 and Threshold-2), RepScope identifies most of the Parler users correctly as bot (human).

Parker (2020) reported that, Parler social network is a platform on which there is no reason for normal people to be there. In other words, Parler users are there for malicious purposes (e.g., conspiracy, political rhetoric). Moreover, in our previous research, we stated that many users of other social networks such as Twitter immigrate to the Parler because of the censorship they experience (Aliapoulios et al., 2021). Therefore, it can be said that Parler users are not concerned about their behavior (e.g., repetition of creating posts in n-consecutive days) and what they post as those on Twitter and other social platforms. Thus, it can be said that Parler users are potentially nonlegitimate or malicious ones avoiding engaging in repetitive behaviors. Therefore, by considering 2 as the value of Threshold-1 and Threshold-2, both the human and bot accounts on Parler (those whose human feature is true and those whose human feature is false) are identified correctly using RepScope. In short, these results show that RepScope achieves a neck-to-neck performance with Botometer on Twitter data by using a small number of simple and platform-independent features. In contrast to RepScope, Botometer's performance relies on more than 1,000 features. Moreover, RepScope achieves high performance not only on Twitter but also on Reddit and Parler social network platforms' data, whereas Botometer could work only on Twitter platform data. Thus, RepScope not only represents an improvement over Botometer but also has the ability to generalize across different social network platforms.

Table 7. Number of repetitions of n-consecutive days and the number of accounts (accounts whose human feature is false and those with human feature of true) that created posts on these n-consecutive days on the Parler dataset

	Number of	
N-Con Rep.	False "Human" Accounts	True "Human" Accounts
0	467	13
2	19	3
3	6	2
4	7	3
5	7	1
6	4	2
7	4	2
8	1	0
9	1	0
10	1	2
11	4	1
12	1	0
16	2	0
21	2	0
22	0	1
25	2	0

CONCLUSION

In this research, we analyzed the behavior of users in sending posts (like tweets on Twitter or submissions on Reddit) on consecutive days and the repetition of this behavior on different data derived from different social networks, including Twitter, Reddit, and Parler. The evaluation results showed that RepScope could successfully identify malicious and nonmalicious behaviors on different social networks. The strength of this method is that it is independent from the features/attributes of different social networks and that it considers only the posts created by users (which are common in nature between different social networks; for example, they are known as tweets in Twitter, submissions in Reddit, and posts in Parler). This feature enables RepScope to be generalizable to different online social network platforms. Moreover, we showed that RepScope could identify bot behaviors correctly, even those that Botometer misses and identifies as humans as demonstrated in the first-round scores collected.

To enhance the performance and accuracy of the RepScope algorithm, there are several avenues for further exploration. One approach is to combine RepScope with other machine learning algorithms, leveraging their complementary strengths to improve the overall detection of repetitive behaviors in social media. By combining different algorithms, we can potentially achieve better performance, as well as better generalization to different datasets. Another promising direction for future work is the integration of RepScope with graph algorithms to further automate the identification and evaluation of repetitive behaviors for user comments and replies. This research can provide deeper insights into the dynamics of repetitive patterns and help uncover coordinated efforts or malicious activities on social platforms. Furthermore, exploring common behaviors among users across various online social networks is an intriguing area of research. By analyzing data from different platforms, such as Twitter, Reddit, and Parler, we can identify patterns that transcend specific networks. This data can lead to a better understanding of human behavior in online environments and potentially uncover overarching trends or strategies employed by bots or coordinated groups across multiple platforms. Overall, by combining RepScope with other machine learning algorithms, integrating it with graph algorithms, and investigating common behaviors across various social networks, we can further advance the detection and analysis of malicious and benign behaviors in online communities.

ACKNOWLEDGMENT

This research was undertaken, in part, thanks to funding from the Canada Research Chairs Program. We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) through the Discovery Grant. The research was conducted as part of the Dalhousie NIMS Lab at https://projects.cs.dal.ca/projectx/ and Dalhousie Persuasive Computing Lab.

COMPETING INTEREST

The authors of this publication declare there are no competing interests.

FUNDING STATEMENT

This research was supported by the NSERC Discovery Grant (RGPIN-2020-04696 and RGPIN-2018-05265).

REFERENCES

Adel Alipour, S., Orji, R., & Zincir-Heywood, N. (2022). Security of social networks: Lessons learned on Twitter bot analysis in the literature. In *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and* Security (pp. 1–9). Association for Computing Machinery. doi:10.1145/3538969.3544450

Aliapoulios, M., Bevensee, E., Blackburn, J., Bradlyn, B., De Cristofaro, E., Stringhini, G., & Zannettou, S. (2021). A large open dataset from the Parler social network. *Proceedings of the International AAAI Conference on Web and Social Media, 15*(1), 943–951. doi:10.1609/icwsm.v15i1.18117

Ashford, J. R., Turner, L. D., Whitaker, R. M., Preece, A., & Felmlee, D. (2020). Assessing temporal and spatial features in detecting disruptive users on Reddit. In *Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp.* 892–896). IEEE. doi:10.1109/ASONAM49781.2020.9381426

Baumgartner, J., Zannettou, S., Keegan, B., Squire, M., Blackburn, J., & Io, P. (2020). The Pushshift Reddit dataset. *Proceedings of the International AAAI Conference on Web and Social Media, 14*(1), 830–839. doi:10.1609/icwsm.v14i1.7347

Brena, G., Brambilla, M., Ceri, S., Di Giovanni, M., Pierri, F., & Ramponi, G. (2019). News sharing user behaviour on Twitter: A comprehensive data collection of news articles and social interactions. *Proceedings of the 13th International Conference on Web and Social Media, 13*(1), 592–597. doi:10.1609/icwsm.v13i01.3256

Costa, A. F., Yamaguchi, Y., Traina, A. J. M., Traina, C., & Faloutsos, C. (2015). RSC: Mining and modeling temporal activity in social media. In *Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 269–278). Association for Computing Machinery. doi:10.1145/2783258.2783294

Cox, K. (2020). *What is Parler, and why is everyone suddenly talking about it?* Ars Technica. https://arstechnica.com/tech-policy/2020/11/what-is-parler-and-why-is-everyone-suddenly-talking-about-it/

Dixon, S. (2022). *Countries with the most Twitter users 2022*. Statista. https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/

Dixon, S. (2023). *Reddit: daily active users 2021–2022*. Statista. https://www.statista.com/statistics/1324264/reddit-daily-active-users/

Echeverrï£¡a, J., De Cristofaro, E., Kourtellis, N., Leontiadis, I., Stringhini, G., & Zhou, S. (2018). LOBO: Evaluation of generalization deficiencies in Twitter bot classifiers. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 137–146). Association for Computing Machinery. 10.1145/3274694.3274738

Gera, S., & Sinha, A. (2022). T-Bot: AI-based social media bot detection model for trend-centric twitter network. *Social Network Analysis and Mining*, *12*(1), 76. Advance online publication. doi:10.1007/s13278-022-00897-6

Hayawi, K., Mathew, S., Venugopal, N., Masud, M. M., & Ho, P.-H. (2022). DeeProBot: A hybrid deep neural network model for social bot detection based on user profile data. *Social Network Analysis and Mining*, *12*(1), 43. Advance online publication. doi:10.1007/s13278-022-00869-w PMID:35309873

Herbert, G. (2020). *What is Parler? 'Free speech' social network jumps in popularity after Trump loses electio*n. Syracuse.com. https://www.syracuse.com/us-news/2020/11/what-is-parler-free-speech-social-network-jumps-in-popularity-after-trump-loses-election.html#:~:text=Parler%20is%20a%20social%20network,allegedly%20emphasizing%20%22free%20speech.%22&text=A%20social%20network%20that%20claims,Trump%20lost%20the%202020%20election

Hurtado, S., Ray, P., & Marculescu, R. (2019). Bot detection in reddit political discussion. In *SocialSense'19: Proceedings of the Fourth International Workshop on Social Sensing* (pp. 30–35). Association for Computing Machinery. doi:10.1145/3313294.3313386

Koggalahewa, D., Xu, Y., & Foo, E. (2022). An unsupervised method for social network spammer detection based on user information interests. *Journal of Big Data*, *9*(1), 7. Advance online publication. doi:10.1186/s40537-021-00552-5

Latah, M. (2020). Detection of malicious social bots: A survey and a refined taxonomy. *Expert Systems with Applications*, *151*, 113383. doi:10.1016/j.eswa.2020.113383

Martin-Gutierrez, D., Hernandez-Penaloza, G., Hernandez, A. B., Lozano-Diez, A., & Alvarez, F. (2021). A deep learning approach for robust detection of bots in Twitter using transformers. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 54591–54601. doi:10.1109/ACCESS.2021.3068659

Martini, F., Samula, P., Keller, T. R., & Klinger, U. (2021). Bot, or not? Comparing three methods for detecting social bots in five political discourses. *Big Data & Society*, *8*(2). Advance online publication. doi:10.1177/20539517211033566

Najari, S., Salehi, M., & Farahbakhsh, R. (2022). GANBOT: A GAN-based framework for social bot detection. *Social Network Analysis and Mining*, *12*(1), 4. Advance online publication. doi:10.1007/s13278-021-00800-9 PMID:34804252

Parker, B. C. (2020). *I tried Parler, the social media app where hate speech thrives*. Sfgate.com. https://www.sfgate.com/tech/article/I-tried-Parler-the-social-media-app-where-hate-15758094.php

Ravazzi, C., Malandrino, F., & Dabbene, F. (2022). Towards proactive moderation of malicious content via bot detection in fringe social networks. *IEEE Control Systems Letters*, *6*, 2960–2965. doi:10.1109/LCSYS.2022.3182291

Saeed, M. H., Ali, S., Blackburn, J., De Cristofaro, E., Zannettou, S., & Stringhini, G. (2021). *TROLLMAGNIFIER: Detecting state-sponsored troll accounts on Reddit*. https://doi.org//arXiv.2112.0044310.48550

Spez. (n.d.). *Reddit's 2017 transparency report and suspect account findings*. Reddit. https://www.reddit.com/user/spez/submitted/

Urbaniak, R., Tempska, P., Dowgiałło, M., Ptaszyński, M., Fortuna, M., Marcińczuk, M., Piesiewicz, J., Leliwa, G., Soliwoda, K., Dziublewska, I., Sulzhytskaya, N., Karnicka, A., Skrzek, P., Karbowska, P., Brochocki, M., & Wroczyński, M. (2022). Namespotting: Username toxicity and actual toxic behavior on Reddit. *Computers in Human Behavior*, *136*, 107371. doi:10.1016/j.chb.2022.107371

Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. In *Proceedings of the Eleventh International AAAI Conference on Web and Social Media (ICWSM 2017)* (pp. 280–289). Association for the Advancement of Artificial Intelligence. doi:10.1609/icwsm.v11i1.14871

Watson, A. (2023). *Social media sites frequently used for news U.S. 2020–2022*. Statista. https://www.statista.com/statistics/330638/politics-governement-news-social-media-news-usa/

Sanaz Adel Alipour is a driven PhD candidate in Computer Science at Dalhousie University, Canada, with a focus on cyber security and data science, specifically within social networks. Her research explores cyber security risks in online social platforms and utilizes data science to extract valuable insights from social network data.

Rita Orji is a Canada Research Chair in persuasive technology and a computer science professor at Dalhousie University, where she directs the Persuasive Computing Lab. Her research is at the intersection of technology and human behavior with a major focus on investigating user-centered approaches to designing technologies to promote social and public goods—specifically, interactive systems to improve lives and support various self-improvement goals. She applies her research to tackle real-life problems in various domains, including improving a wide range of health and wellness objectives, such as promoting mental health, and discouraging risky health behaviors, including risky sexual behaviors, smoking cessation, promoting safety, security, and environmental sustainability.

Nur Zincir-Heywood is a Distinguished Research Professor and an Associate Dean Research of the Faculty of Computer Science with Dalhousie University, Canada. She is the Co-Editor of the books Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning (Wiley/IEEE), and Recent Advances in Computational Intelligence in Defense and Security (Springer) as well as the coauthor of the book Nature-Inspired Cyber Security and Resiliency: Fundamentals, Techniques, and Applications (IET). Her research interests include machine learning and artificial intelligence for cyber security, network, systems, and information analysis, topics on which she has published over 200 fully reviewed papers. She is a recipient of several best paper awards as well as the Supervisor for the recipient of the IFIP/IEEE IM 2013 Best Ph.D. Dissertation Award in Network Management. She is an Associate Editor of the IEEE Transactions on Network and Service Management, International Journal of Network Management (Wiley), and Journal of Network and Systems Management (Springer).