Are Bots Humans? Analysis of Bot Accounts in 2019 Indian Lok Sabha Elections

by

Hitkul ., Omkar Gurjar, Aanshul Sadaria, Kanay Gupta, Shashank Srikanth, Rajiv Ratn Shah, Ponnurangam kumaraguru

in

IEEE Sixth International Conference on Multimedia Big Data (BigMM)
: 1
-10

New Delhi

Report No: IIIT/TR/2020/-1

Centre for Language Technologies Research Centre
International Institute of Information Technology
Hyderabad - 500 032, INDIA
September 2020

Are Bots Humans? Analysis of Bot Accounts in 2019 Indian Lok Sabha Elections (Workshop Paper)

Hitkul*, Omkar Gurjar†§, Aanshul Sadaria†§, Kanay Gupta†
Shashank Srikanth‡, Rajiv Ratn Shah* and Ponnurangam Kumaraguru*
**IIIT- Delhi,*†*IIIT- Hyderabad*
**(hitkuli,rajivratn,pk)@iiitd.ac.in*
†*(omkar.gurjar, aanshul.sadaria, kanay.gupta)@students.iiit.ac.in*
‡*shashank.s@research.iiit.ac.in*

***Abstract*—Social media platforms have taken political and cultural conversations to an online platform making them more accessible. Ability to anonymously post has allowed more people to participate fearlessly. However, this has also led to an opportunity to spread miss information and manipulative content. Political groups around the globe have used Bot accounts to help spread their preferred narrative online during elections. In the midst of 2019 Indian Lok Sabha Elections speculations were made about the presence of cyber-troops/IT Cells which operate fake accounts and push propaganda. Our finding suggests that a portion of Bot accounts seems to be operated by humans in the background. These accounts have a very distinct usage pattern on Twitter compared to legitimate human users. Our experiments also point out that only 1.3% of total interactions are directed from Humans to Bots, showing Bot accounts inability to gel well in the online social network.**

***Keywords*-Social Networks, Bots, Twitter, Elections**

I. Introduction

Social Media have become a new hub of democratic conversations online [1], [2], [3]. This has helped in increasing the participation in the conversation by a lot, but the possibility of manipulation and misinformation is equally real [4], [5]. The resurgence of Twitter use for elections have been observer in multiple countries like the USA [6], Germany [7], France [8]. As the campaign for 2019 Indian Lok Sabha Elections started, India experienced a similar rise in political conversations of Twitter. #LokSabhaElections2019 became one of the top three most used hashtag on Twitter in the first half of 2019 [9]. However, with a high reach of a platform comes the high possibility of manipulation and spreading miss information [10].

Twitter bots have been used repeatedly in an election as an online opinion manipulation tool. A Bot is a social media account, controlled predominantly or completely by a software [11]. The evidence of using Bots to manipulate elections dates back to 2010 [12]. This subject received an vast popularity after the 2016 US Presidential election [6], [13], [14] and since then the role of bots has been studied in The US Midterm [15], [16], [17], Germany's Federal election [18], [7], French presidential election [8] to name a few.

[19] pointed out the usage of cyber-troops or *IT Cells* by Indian political parties to manipulate their perception via social media. IT Cells of political parties is an organization built to frame a favourable narrative for the political party online. People working for IT Cell create fake social media accounts which aim to camouflage in a sea of users and push their manipulative narrative.

Even though the vast literature on bots and election exist, not much work has been done in understanding who is behind the bot accounts. In this paper, we look at the device and usage pattern of accounts to uncover *if bot accounts all algorithmic or operated by humans*. Then we look at the temporal, metadata and content analysis to understand *how bot behaviour was different from humans* in the context of 2019 Indian election. Finally, we look at the analysis of interactions between bot and humans to understand *how inter-mixed bots are with humans* on the election-related online conversations.

Rest of this paper is organized in the following manner. Section II talks about the previous literature studying the role of bots in elections. Section III mentions the details of our data collection and methodology to labels users as bots or humans. Section IV has three major subsections, each answering one of our research questions. Finally, we point out some limitations of this study in Sections V and conclude the paper in Section VI.

II. Related Work

The role of bots on elections have been documented widely in the literature. A set of seed studies emerged from The 2016 United States Presidential Election [6], [13], [14]. Since then similar effects has been studied on The 2018 United States Midterm Election [15], [16], [17], Germany's Federal Election [18], [7], French Presidential Election [8]. Apart from election, research have shown effect of bots on word wide events across domain [11], example Catalan referendum [20] and COVID-19 pandemic [21]. In this

§Equal contribution

978-1-7281-9325-0/20/$31.00 ©2020 IEEE
DOI 10.1109/BigMM50055.2020.00073

work we will focus on the literature available in context of elections.

[6] analysed the twitter data from The 2016 US Presidential election and found bots are responsible for creating polarisation, spreading miss information and redistributing influence in the network for achieving a malicious purpose. [13] proposed a novel algorithm to quantify user/bot influence and found that bots can be biased towards one political party. This finding was in line with what was demonstrated by [15]. Further [16] analysis of the US Midterm election debate pointed out that removing bot tweets does not affect the outcome; however, removing retweet can lead to a more significant effect.

More recently, [20] demonstrated that even after the sophisticated algorithm used for the development of bots, they fail to gain a central position in the network and interaction with human users are very limited. On the same line, [21] study of the ongoing COVID-19 pandemic demonstrates content produced by bots are far more propagandist compared to humans, and there is a vast behaviorally difference among the two groups.

A large volume of literature discusses the behaviour of bots amid worldwide events. Limited work explores the nature of the entity behind these bots.

III. Data Collection and Bot Detection

The Lok Sabha election 2019 in India took place in seven phases, each responsible for polling in one region of the country. The seven phases were distributed over approximately a month starting from 11 April 2019 and ending on 19 May 2019. Finally, on 23 May 2019, the election results were declared. Since the election-related discourse on social media spans before and after the election dates, our data collection was done from 5 February 2019 (two months before first polling) to 25 June 2019 (one month after results).

We handcrafted a list of hashtags related to the 2019 Lok Sabha election. The list was updated on an hourly basis to include new election-related trending hashtags. The update window was reduced to fifteen minutes on the seven days of voting. In the end, we had a list of $3,698$ hashtags. Twitter's Streaming API was used to continuously collect posts, including a hashtag from the list. Further, we continuously queued Twitter's Search API to collect any data which may have been missed by Streaming API due to its limitations [22].

We collected a total of 45.6 million tweets, made by 2.2 million unique users. Out of the total data, 7.4 million were original tweets. 1.9 million were quoted Tweets (also known as retweet with text), and 35.8 million were retweets. When observed, we discovered discrepancies in hashtag usage patterns. For example, spaces present between # symbol and text - '# election' or no spacing between consecutive hashtags - '#election#loksabha'. Twitter's default hashtag parser does not account for these errors. To this end, we wrote a custom regex to filter out these hashtags. Post filtering, there were a total of approximately 1 million unique hashtags in the data. The dataset can be requested from our website.[1]

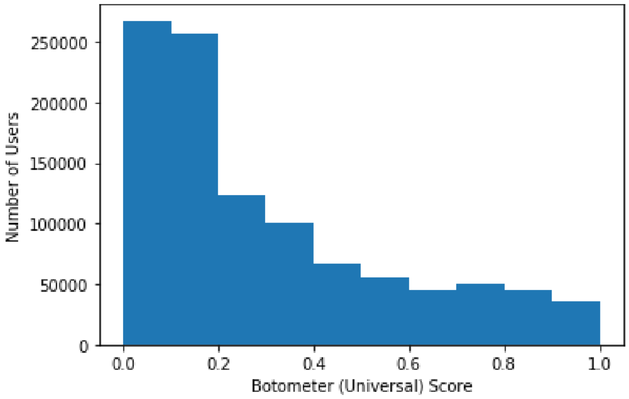


Figure 1: Distribution of Botometer score for 1,046,260 users

A. Bot Detection

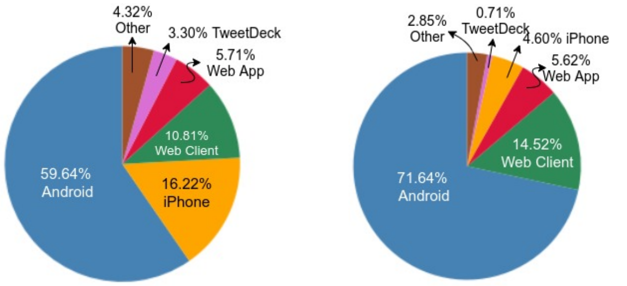
We decided to use the Botometer API [23] to classify users into the *Bots* or *Humans* due to its popularity in literature [6], [24], [11] and continuous improvements [25]. The Botometer API provides a score (hereafter referred as Botmeter score) between 0 and 1 for every user. Furthermore, the API provides two versions of the Botometer score, 'English' better suited for Tweets done in English language and 'Universal' which is language agnostic. Since our data has a host of Indian regional languages, we use the 'Universal' score in this study. Due to API constraints, we were only able to get Botometer score for 1 Million users (50% of total users in our dataset). To the best of our knowledge, ours is one of the largest analysis in terms of the number of users annotated by Botometer API with [21] being the only other comparable study. Figure 1 shows the distribution of Botometer score for our data.

A standard way to classify users into *Bots* or *Humans* is by setting a threshold of 0.5 on Botometer score [6]. This method labels 0.8 million users as *Humans* and 0.2 million users as *Bots*. However, doing a blind threshold at 0.5 can lead to errors. Instead, we decided to use users who lie in the top and bottom ten percentile of our Botometer score distribution as suggested by [21]. This reduces the possibility of classification error significantly by only picking users with high confidence *Bot* or *Human* score. By employing this method, we finally have 104,626 users for each class. For the rest of this paper all the experiments are done on these set of users. Table I shows statistics about the dataset.

[1] http://precog.iiitd.edu.in/requester.php?dataset=elections19

Table I: Summary of dataset statistics

Total Tweets	45,620,337
Number of original tweets	7,410,088
Number of quoted tweets	1,989,896
Number of retweets	36,220,353
Number of unique hashtags	999926
Number of unique users	2,209,217
Number of users test by Botometer API	1,046,260
Number of Bots (Botometer score >0.5)	231084
Number of Humans (Botometer score <0.5)	815176



(a) Human's device makeup

(b) Bot's device makeup

Figure 2: Device makeup for humans and bot accounts. Both groups have largest proportion of traffic coming from Android phones, which is an indicator of that bots are actually humans.

IV. Data Analysis

Political groups around the world have been using social media propaganda and bots to gain strategic advantage [26]. Effect of Twitter bots on elections have been studied widely. Some of the examples are - The 2016 United States Presidential Election [6], [13], [14], The 2018 United States Midterm Election [15], [16], [17], Germany's Federal Election [18], [7], French Presidential Election [8] and large political events around the world [20], [21], [27].

We aim to study the effect of bots in the 2019 Indian Lok Sabha Election. Though we suspect many behavioural traits will be similar to the ones observed in other studies (see Section IV-B), near elections reports and news articles started pointing out heavy use of *cyber-troops* or more popularly know as *IT Cell* by political parties to manipulate campaign [19], [28]. IT cells are a group of people who help in spreading misinformation or propaganda using fake accounts. These accounts can be fully autonomous, manual or a combination of both. Theoretically, fake accounts operated by humans should be better at camouflaging them as a legitimate account in order to fool other users and the platform's blocking algorithm. Based on this we aim to answer three questions via our analysis:-

- *RQ1: Are bots actually humans?*
- *RQ2: How is bot behavior different from humans?*
- *RQ3: Do bot users succeed in camouflaging as human users?*

A. Are bots actually humans?

Two major points of operating differences between manually operated and algorithmic accounts are usage pattern and interaction medium with the platform. Though the majority of humans browse social media via smartphones, algorithmic bots would need to use the platform's API to perform actions [29]. Secondly, usage patterns of bots are different from humans as algorithms are not affected by which day of the week or hour of the day it is.

1) Tweeting device makeup: Tweet object served by Twitter API contains the information of the device used to create the tweet. Figure 2 shows the device makeup for human and bot users. For human users, the distribution is as expected. Android owns the largest share, then iPhone followed by various web clients and a minuscule amount of traffic coming from other unknown sources. However, results from bots were surprising. Previous research clearly shows that the majority of bot traffic comes from API [29], though in our case three-quarters of the traffic is coming from Android phones. This indicates that real people operate the bot accounts. Another interesting finding is the traffic from the iPhone is less compared to the web in case of Bots. This can be explained by the fact that iPhone's are notably expensive in India, and hence financially, it is sensible for the IT Cell administration to provide cheap Android phones/computers to the operators.

2) Tweeting Pattern: Humans tweeting entropy is low as they have a fixed pattern of using social media platform. Humans tweeting frequency should reduce later in the evening, whereas bot frequency remains relatively high [29]. Figure 3 visualizes a heat map of tweets done on every minute and hour of the day by humans and bots. The most important insight in this figure is the randomness in tweeting pattern of bots. This behaviour is expected. Bots are not bounded by day-to-day chores and can keep on pushing the agenda on Twitter. At the same time, humans have precise times when they can spend extended time on social media.

An unexpected behaviour here is the high activity of bots in the mornings and sudden drop in activity during the evening. To better understand this behaviour, we plot Tweet frequency by the hour of the day in Figure 4. Humans tweeting frequency increase in the early hours and take a dip from 0800 to 1300 hours (typical working hours). Humans tweet the most between 1500 to 1700 hours which is the time frame between the end of work hours and dinner time. This is expected as those are the hours of the day when most people are free from both work and family obligations.

Typically autonomous bots follow a constant tweet frequency though out the day [29], but that is not true in our case. The pattern in aspects is the reverse of what humans

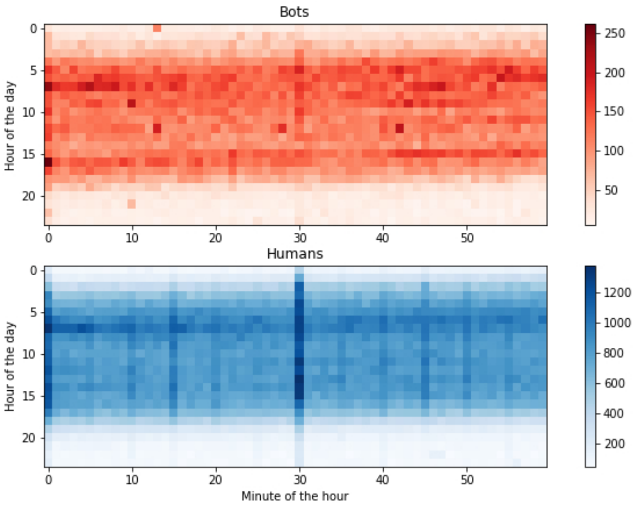


Figure 3: Heat map of number of tweets done for hour of the day and minute of the hour.

follow. In our data, bots tweeting frequency increases early in the morning, peaking around 600 hours, maintains though out the morning and afternoon and then falls steeply after 1500 hrs.

This leads to two crucial insights - 1) Since, most users check Twitter at least once before the work, reaching peak frequency early morning can help populate the Twitter feed of content IT Cell wishes to propagate and 2) Early morning peaks and a sudden drop after 1500 hours shows a typical 8-9 hour work cycle which humans will follow, but there is no reason why an autonomous bot needs to do it.

Combining the insights gained from Tweeting device distribution and entropy, it is clear that real humans operate a sizable proportion of our bot users. These people are part of *Cyber Troops* or *IT Cells*. They aim to create fake/dummy user accounts and push propaganda on social media platforms. Next, we study hows the behaviour of these bots/suspect users differs from the behaviour of legitimate human users.

B. *How is bot behavior different from humans?*

A possible advantage of using humans to operate propaganda accounts should be their organic and natural human behaviour. That should help them in mixing well with legitimate users on the platform and avoid flagging algorithms deployed by Twitter. On the contrary, IT Cell operators are instructed about the agenda they have to put forward and how. This can lead to artificial behaviour. In this section, we study comparisons between bots and humans based on temporal analysis, user metadata and content posted.

1) Temporal Analysis: Figure 5 provides the temporal distribution of tweets done by humans and bots during the timeline of data collection. In general, humans produce more traffic comparison to bots. Clear peaks can be observed in human traffic during each voting phase and on the result day, but bot traffic shows a few undulations barely from the mean behaviour. This can be possibly explained by the fact that humans are more sensitive to get engaged in online political discourse as a consequence of an event in the offline world. On the other hand, bots are trained to slowly and steadily push their agenda over time [6].

To further extend the temporal analysis, we look into the traffic for the individual type of post - Tweets, Retweets, Replies and Mentions. For each type, we calculate Volume of post per minute and percentage of content produced by bots over humans for the entire timeline of our data collection. Results of these analysis are shown in Figure 6 and Figure 7 respectively.

As observed from Figure 6, the activity of bots before the start of elections is minuscule. This indicates that these accounts were created especially for discourse during the election. Furthermore, humans tend to Mention and Reply a lot more in comparison to bots. This can be an indicator of the bots inability to engage in long-form social discourse. These insights are further reinforced by Figure 7. On average, only 1.29% Mentions and 5.39% Replies are produced by bots.

In the conclusion of the temporal analysis, we can say that humans tend to engage in two way social discourse on Twitter and their usage patterns are affected by political events in the offline world. On the contrary, bots tend to consistently push their agenda with time using one-way strategies like retweets and tweets irrespective of online/offline events.

2) Metadata Patterns: In this section, we look at the age and account reputation [29] of users to gain insights into users timeline and social standing on the platform. We calculate the age of a user as the delta between account creation date and 10 April 2019 (Phase 1 voting day). Figure 8 provides a distribution for age (in days) for bot and human users. In line with the observations of literature [21], most bot accounts in our dataset were created just before the elections. The median age for a bot account is 178 days, which is 14 times less than the median age of human users (2516 days). Starting a new account and jumping straight into regular political discourse shows a sign of suspicious behaviour, especially during the time of elections.

Next, we look at users reputation score to gain insights into the network connections of the user. Twitter provides an option to 'Follow' other users. People who follow you can see your tweets. Additionally, if two people follow each other, they are known as Friends. Legitimate human accounts tend to have a linear relationship between followers and friends [29]. One notable exception to this rule is celebrities. Famous accounts tend to have a very high number of following and a little number of friends. For example, at the time of writing this paper, Prime Minister Narendra Modi is followed by 60.3 Million people but only has 2,352 friends.

Bot accounts face a problem which is opposite to the one

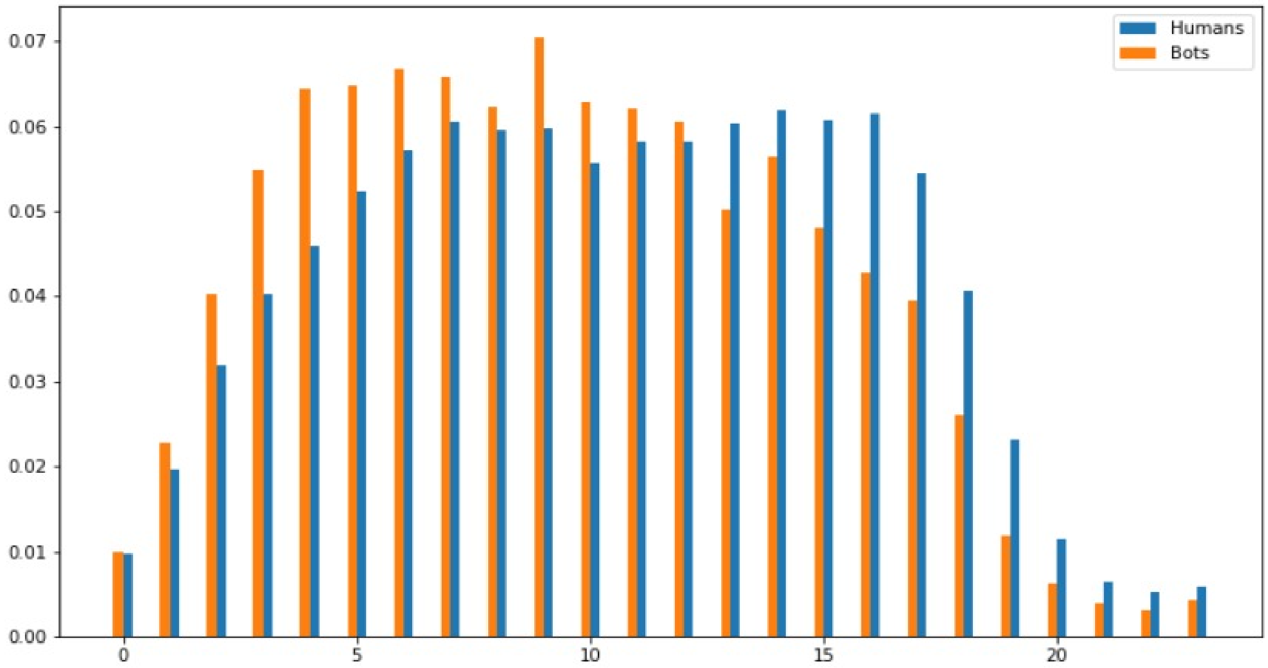


Figure 4: Frequency of Tweets compared with Hour of the day. Bot's tweeting behavior matches closely to typical working hours.

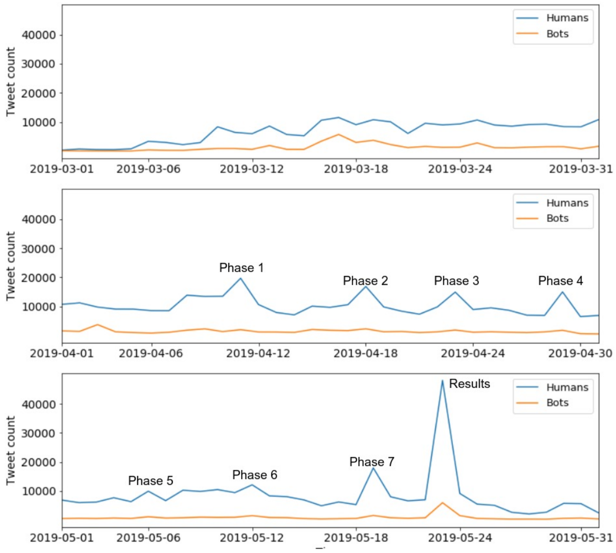


Figure 5: Volume of Tweets generated by Humans and Bots during the collection period

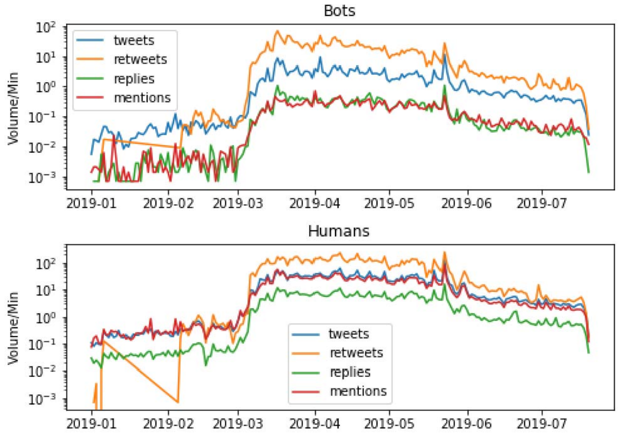


Figure 6: Volume per minute for different types of Twitter posts.

observed in celebrities. They tend to follow a large number of users to increase their reach, but due to their unsolicited nature, people rarely follow them back (become friends). When Twitter started flagging down these kinds of account, Bots became more sophisticated and started unfollowing the people who do not follow them back [29]. This behaviour leads to approximately 1:1 ratio of friends and followers, which is too unlikely for legitimate users. Accounting for all these features, [29] proposed a score called *Account Reputation* (AR) to rate reputation of a user on Twitter. Refer Equation 1 for the mathematical formulation of the score.

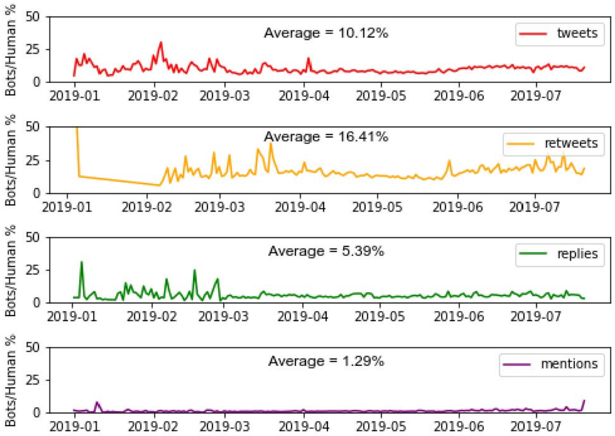


Figure 7: Percentage of traffic generated by Bots for different type of Twitter posts.

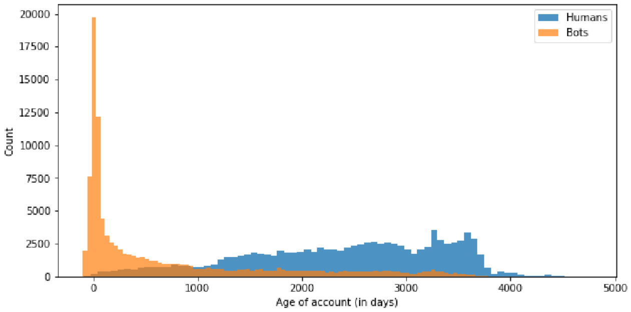


Figure 8: Histogram of age of accounts. Majority of bots joined the platform just before the election started.

$$AR = \frac{followers\_no}{followers\_no + friends\_no} \tag{1}$$

AR score tends to 1 for popular/reputed people ($followers\_no >> friends\_no$) and 0 for bots ($followers\_no << friends\_no$). Figure 9 shows a Cumulative Frequency Distribution (CDF) of AR for bot and human users in our dataset. For a given AR score of x, its CDF tells us the probability of AR scores being $\leq x$. Figure 9 indicates that the probability of bot accounts having a low AR is disproportionately higher as compared to humans.

In conclusion, after looking at a metadata, we can claim that majority of the bot accounts are created very close to the elections and do not hold a very high AR score.

3) Content Analysis: Lastly, in this section, we look at the differences in content posted by bots and humans if any. In this study, the scope of content analysis is limited to hashtags only, but this can be extended by analysing other content factors like sentiment [30], LIWC [31], language.

Table II enumerates the top ten hashtags used by the bot and human accounts. Only two out of ten hashtags used by humans are related to a specific candidate but, six out of ten most frequently used hashtags bots are related to a political party, candidate or agenda.

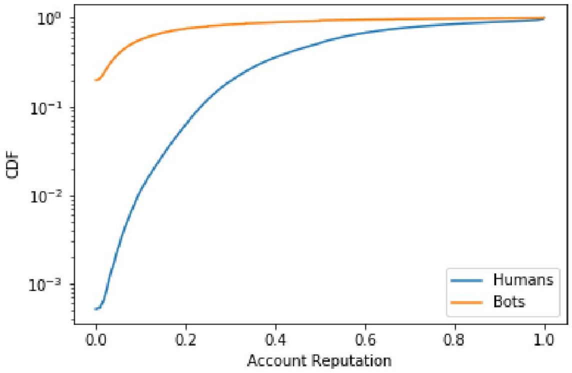


Figure 9: CDF of account reputation. Bots have a approximately 100 times more probably to have a low account reputation compared to humans.

Table II: Top 10 distinctive hashtags used by bots and humans.

Top 10 hashtags used by bots	**Top 10 hashtags used by humans**
justiceforebiz	ElectionsWithNews18
congress	ElectionsWithHT
modi	ElectionsWithTimes
india	Verdict2019
GrowSouthAfrica	RahulGandhi
Peoplemanifesto	IndiaElections2019
bjp	BattleOf2019
narendramodi	ExitPoll2019
politics	PhirEkBaarModiSarkar
elections2019	LokSabhaElection2019

We calculated the Coefficient of Traffic Manipulation (CTM) [32] for all hashtags, which occurred more than 1,000 times in our dataset. CTM is a relative metric to measure how much traffic of a given hashtag has been manipulated on Twitter. Equation 2 provides an mathematical representation of CTM.

$$C = \frac{R}{100} + F + U \tag{2}$$

Here, For a given hashtag t:-

- C is Coefficient of Traffic Manipulation for t.
- R is percentage of t traffic created by retweets.
- F is percentage of t traffic created by top fifty users.
- U is average number of tweets per user for t.

Top ten uniquely used hashtags by top and bottom decile users qualified for the CTM calculation. Average CTM score was 40.02 and 20.6 for hashtags uniquely used by the bot and human accounts, respectively. This means the on average bot traffic is 1.95 times more manipulated then traffic generated by human accounts.

In conclusion, it is fair to mention that clearly bot accounts manipulate traffic multiple folds as compared to human accounts and post content which is trying to push forward and agenda/ideology.

By combining the conclusions of large scale temporal, metadata and content analysis, it can be seen that Twitter behavioural patterns of bot users are widely different from that of humans, even though in the background the bot accounts may be operated by humans. A possible explanation for this can be if the account operators are strictly instructed on what content to push and how, it makes the accounts very one dimensional and algorithmic. Moreover, since most probably all the IT Cell operators receive the same set of instructions, it makes the behaviour widespread and much easier to detect.

Next, we explore the interactions between the bot and human accounts to assess if humans can notice these behavioural differences of bot accounts and maintain distance from them as shown in [20] or these difference are not noticeable during the day to day use, and the human-operated fake accounts being able to deceive the legitimate users.

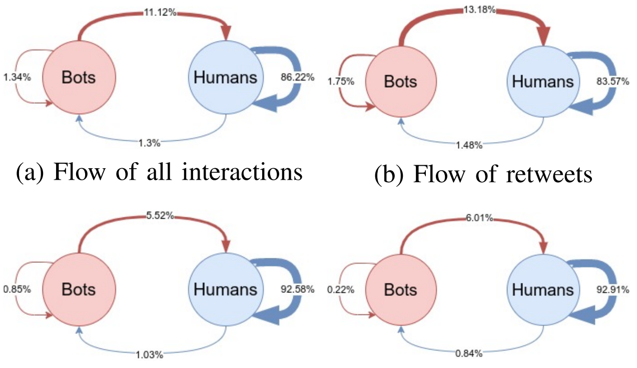
C. Do bot users succeed in camouflaging as human users?

Initially, we build a directed graph of all the interactions between our top and bottom decile Botometer score users. In our directed graph, users represent nodes, and a directed edge represents each interaction. An edge from node A to node B means user A interacted with user B. Retweet, reply or mention counts as interactions in our experiment. Our graph had a total of 209,252 nodes and 14,008,245 (14 Million) edges.

Figure 10 shows an overview of how interactions occur between different types of nodes. We observe a consistent pattern of bot accounts, trying to interact with human accounts (5% to 14%). However, majority system interactions (90%) occur between human accounts.

Building over the previous analysis, we calculated complementary cumulative distribution function (CCDF) for the retweet interactions between humans and bot. CCDF is reverse of CDF. Given a value x, CCDF indicates the probability of a random variable getting value higher than x. Checking CCDF of interactions also gives us a more detailed quantitative insight on how interactions are taking place.

Figure 11 shows the CCDF for retweets done by humans and bots. For each graph, we calculate three distributions, in the group (bot-bot, human-human), across the group (bot-human, human-bot) and everyone (bot-all, human-all). Perhaps the most exciting finding is that bots are more probable to retweet a human compared to other bots, but on the other hand probability of a human user retweeting a bot is quite small as compared to the probability of a



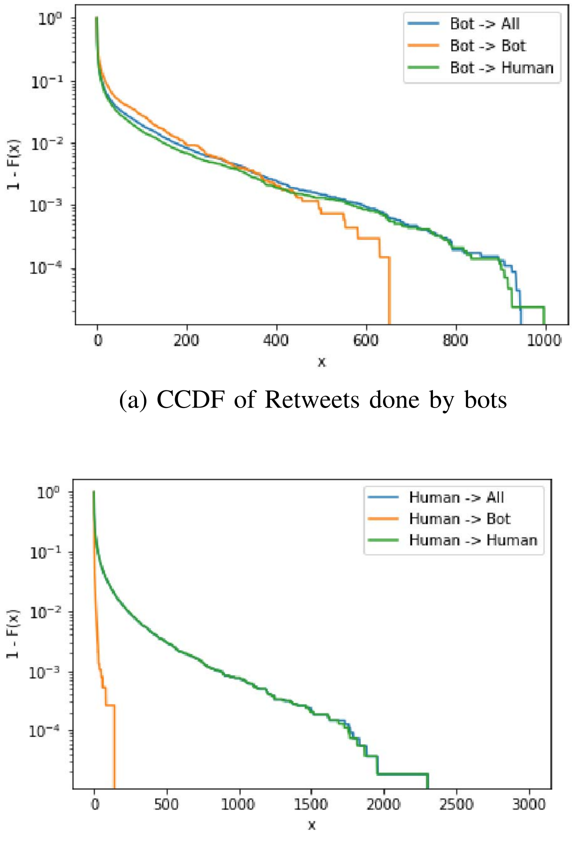
(a) Flow of all interactions

(b) Flow of retweets

(a) Flow of quotes

(b) Flow of mentions

Figure 10: Flow of interactions between bot and human accounts. Bot accounts consistently try to interact with human accounts and fail.



(a) CCDF of Retweets done by bots

(b) CCDF of Retweets done by humans

Figure 11: CCDF of retweets done by bots and humans. Probability of bots retweeting other bots or humans retweeting a bot is multiple folds smaller then human-human or bot-human interactions.

human retweeting other humans. This observation is very different from what was observed in the 2016 United States Presidential election where retweets within and across the group were very identical [6]. This leads us to speculate that probably the strategies employed by IT Cells during Indian election were not as sophisticated as employed in The US election. The sheer difference between the majority and minority interaction is worth noting. Minority retweet (bot-bot and human-bot) are so insignificant in number that the distribution of majority retweet (bot-human, human-human) almost exactly overlaps the distribution of total retweets in both cases. This indicates the total desperation of bots to interact with humans and complete rejection of bots by humans.

We replicated the same analysis for replies interactions too, and the results indicated precisely the same pattern of retweet CCDF. Those graphs are not included in the paper due to space constraints.

Lastly, to study the position and importance of nodes in our graphs, we calculate the PageRank [33] centrality for every node. A higher PageRank value means that the nodes hold a more *Central* position in the graph. For our interactions graphs, PageRank of human users was 1.36 times more than that of bot users on an average. This means that humans hold a more central/important position in the network, whereas bots stay on the periphery of the social system.

Accounting for the limited interactions with human accounts and a lower network PageRank it is safe to conclude that the IT Cell operated accounts fail to diffuse with the legitimate human accounts. Even though real humans operate the accounts themselves, fake identity and drastic difference in usage behaviour get notices quite quickly. This leads the suspected/bot/IT Cell accounts holding a relatively weaker position on the Twitter social network.

V. Limitations

Our study has two significant limitations. Firstly, our dataset was collected using the free tier of Twitter API. Streaming API only provides exposure to 1% of the total traffic on Twitter. To eliminate that effect, we use Twitter Search API in conjunction, but our data collection pipeline still may be susceptible to the biases of over-represented topics [22].

Our second limitation is using Botometer for labelling the accounts as bots or humans. Despite the popularity and state-of-the-art performance of standard datasets, any machine algorithm is susceptible to error when used in a real-time scenario. This can have a pronounced effect on our data as most of the data is coming from India, and the standard dataset is collected mainly from western Twitter. This means many value distribution of some features which Botometer uses like the *likelihood of screen_name* [25] in our data be very different from western data which can confuse the model. We believe many of these errors will be suppressed by the sheer size of our data and experimenting only on the bottom and top decile users, but the possibility of bias persists.

An extension of second and perhaps the most significant limitation of our paper can be using Botometer to mark IT Cell operated Bot account. Even though analysis in Section IV shows indications of labelled Bot accounts being operated by real people and failing to interact with Human accounts; possibly a portion of IT Cell operated Bot accounts are camouflaged too well to be spotted by Botometer. That said, the study still points out some clear indication of suspected user activities in the data and to better understand and fill in the limitations further research is required. A dipper examination of these accounts is required to understand the properties and categorize these accounts. It is also necessary to conduct an experiment (automated and manual) independent of Botometer to understand better the deficiency of the system and its ability to classify people operated bot accounts.

VI. Conclusion

Our paper aims to study the bot users deployed on Twitter during the 2019 Indian Lok Sabha election. A total of 45.6 Million tweets done by 2.2 Million unique users are collected by querying Twitter Search and Streaming API with a handcrafted list of election-related hashtags. Approximately 50% (1 Million) randomly sampled users are annotated as a bot or human using the Botometer API. This makes it one of the most extensive studies in terms of accounts which are annotated by the Botometer API. Probing the user device and entropy Bot accounts uncover that a sizeable portion is fake accounts operated by real people. This affirms the presence of an IT Cell/Cyber troop. In theory, this should make it reasonably trivial for suspected users to merge with legitimate users on social media and start pushing propaganda. Though, detailed analysis of bot account behaviour shows drastic differences in the usage pattern compared to humans. As expected, uni-dimensional instructed usage pattern of IT Cell Bot accounts, get noticed by legitimate human accounts, ultimately leading to minimal interactions between the two. Alongside with the limitations mentioned in Section V, it is essential to point out that an inability to hold a central position in social media network does not mean that these accounts do not create undemocratic harms to the election process. Future work can focus on isolating its effect of bot accounts on the Indian election and better categorization of IT Cell accounts.

References

[1] O. Varol, E. Ferrara, C. L. Ogan, F. Menczer, and A. Flammini, “Evolution of online user behavior during a social upheaval,” in *Proceedings of the 2014 ACM conference on Web science*, 2014, pp. 81–90.

[2] M. T. Bastos, R. Recuero, and G. Zago, "Taking tweets to the streets: A spatial analysis of the vinegar protests in brazil," *First Monday*, vol. 19, no. 3, 2014.

[3] C. Beaumont. Mumbai attacks: Twitter and flickr used to break news, bombay india - telegraph. [Online]. Available: https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html

[4] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, S. Patil, A. Flammini, and F. Menczer, "Truthy: mapping the spread of astroturf in microblog streams," in *Proceedings of the 20th international conference companion on World wide web*, 2011, pp. 249–252.

[5] J. Ratkiewicz, M. D. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. M. Menczer, "Detecting and tracking political abuse in social media," in *Fifth international AAAI conference on weblogs and social media*, 2011.

[6] A. Bessi and E. Ferrara, "Social bots distort the 2016 us presidential election online discussion," *First Monday*, vol. 21, no. 11-7, 2016.

[7] F. Morstatter, Y. Shao, A. Galstyan, and S. Karunasekera, "From alt-right to alt-rechts: Twitter analysis of the 2017 german federal election," in *Companion Proceedings of the The Web Conference 2018*, 2018, pp. 621–628.

[8] E. Ferrara, "Disinformation and social bot operations in the run up to the 2017 french presidential election," *arXiv preprint arXiv:1707.00086*, 2017.

[9] N. Mathur. Twitter celebrates 12th birthday of the 'hashtag'. [Online]. Available: https://www.livemint.com/companies/news/twitter-celebrates-12th-birthday-of-the-hashtag-1566546599327.html

[10] P. N. Howard *et al.*, *New media campaigns and the managed citizen*. Cambridge University Press, 2006.

[11] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Communications of the ACM*, vol. 59, no. 7, pp. 96–104, 2016.

[12] P. T. Metaxas and E. Mustafaraj, "Social media and the elections," *Science*, vol. 338, no. 6106, pp. 472–473, 2012.

[13] M.-A. Rizoiu, T. Graham, R. Zhang, Y. Zhang, R. Ackland, and L. Xie, "# debatenight: The role and influence of socialbots on twitter during the 1st 2016 us presidential debate," in *Twelfth International AAAI Conference on Web and Social Media*, 2018.

[14] N. Abu-El-Rub and A. Mueen, "Botcamp: Bot-driven interactions in social campaigns," in *The World Wide Web Conference*, 2019, pp. 2529–2535.

[15] K.-C. Yang, P.-M. Hui, and F. Menczer, "Bot electioneering volume: Visualizing social bot activity during elections," in *Companion Proceedings of The 2019 World Wide Web Conference*, 2019, pp. 214–217.

[16] A. Deb, L. Luceri, A. Badaway, and E. Ferrara, "Perils and challenges of social media and election manipulation analysis: The 2018 us midterms," in *Companion proceedings of the 2019 world wide web conference*, 2019, pp. 237–247.

[17] L. Luceri, A. Deb, A. Badawy, and E. Ferrara, "Red bots do it better: Comparative analysis of social bot partisan behavior," in *Companion Proceedings of the 2019 World Wide Web Conference*, 2019, pp. 1007–1012.

[18] T. R. Keller and U. Klinger, "Social bots in election campaigns: Theoretical, empirical, and methodological implications," *Political Communication*, vol. 36, no. 1, pp. 171–189, 2019.

[19] U. Campbell-Smith and S. Bradshaw, "Global cyber troops country profile: India." [Online]. Available: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf

[20] M. Stella, E. Ferrara, and M. De Domenico, "Bots increase exposure to negative and inflammatory content in online social systems," *Proceedings of the National Academy of Sciences*, vol. 115, no. 49, pp. 12 435–12 440, 2018.

[21] E. Ferrara, "What types of covid-19 conspiracies are populated by twitter bots?" *First Monday*, May 2020. [Online]. Available: http://dx.doi.org/10.5210/fm.v25i6.10633

[22] F. Morstatter, J. Pfeffer, H. Liu, and K. M. Carley, "Is the sample good enough? comparing data from twitter's streaming api with twitter's firehose," in *Seventh international AAAI conference on weblogs and social media*, 2013.

[23] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, "Botornot: A system to evaluate social bots," in *Proceedings of the 25th international conference companion on world wide web*, 2016, pp. 273–274.

[24] O. Varol, E. Ferrara, C. A. Davis, F. Menczer, and A. Flammini, "Online human-bot interactions: Detection, estimation, and characterization," in *Eleventh international AAAI conference on web and social media*, 2017.

[25] K.-C. Yang, O. Varol, P.-M. Hui, and F. Menczer, "Scalable and generalizable social bot detection through data selection," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 01, 2020, pp. 1096–1103.

[26] S. Bradshaw and P. N. Howard, "The global disinformation order 2019 global inventory of organised social media manipulation." [Online]. Available: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[27] D. Stukal, S. Sanovich, R. Bonneau, and J. A. Tucker, "Detecting bots on russian political twitter," *Big data*, vol. 5, no. 4, pp. 310–324, 2017.

[28] S. SIRUR, "India among 70 nations hiring 'cyber troops' for propaganda, says oxford university study," *The Print*, Sep 2019. [Online]. Available: https://theprint.in/india/india-among-70-nations-hiring-cyber-troops-for-propaganda-says-oxford-university-study/299042/

[29] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?" *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 811–824, 2012.

[30] C. J. Hutto and E. Gilbert, "Vader: A parsimonious rule-based model for sentiment analysis of social media text," in *Eighth international AAAI conference on weblogs and social media*, 2014.

[31] Y. R. Tausczik and J. W. Pennebaker, "The psychological meaning of words: Liwc and computerized text analysis methods," *Journal of language and social psychology*, vol. 29, no. 1, pp. 24–54, 2010.

[32] B. Nimmo, "Measuring traffic manipulation on twitter," 2019.

[33] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," 1998.