

Social BOT Detection for Twitter Dataset by User Action and Genetic Algorithm

Sanjay Soni, Dr. Ritu Shrivastava

SIRTS

Bhopal (M.P.), India.

Sanjaysoni160@gmail.com

Abstract- Digital platform dependency of today era attract promoters to brand product services. So unwanted posting was done by some programs known as bot. Number of researchers have proposed different techniques to identify these bots which was post by bot programs. This paper has developed a model to identify bots from real user. User action were analyze as features for classification of bots and real user. Whole process adopt graph based clustering and teacher learning based optimization genetic algorithm. Graph based clustering classify user into two class and genetic algorithm find the class representative action sequence in form of features. Experiment was done on real twitter dataset and result shows that proposed model has increase the detection accuracy of work.

Keywords- Clustering, Data mining, Genetic Algorithm, Social Network, Online Social Networks (OSNs), Twitter, Spammers, Legitimate users

I. INTRODUCTION

Social networks are very well-known networks through which data or thoughts of individual or community are exchanged across the globe. A social organization is formed of nodes that are normally entities or associations. Individuals are communicating in Social Networks and developing relationships with one another. In Social Networks websites like Facebook, twitters, my web space and LinkedIn are highly liked websites. Millions of clients, are fascinated with these websites and many of them have taken these websites as part of their living. From the past some years, the Social Networking websites like Facebook, twitter. LinkedIn etc. have achieved so much recognition as it becomes the everyday routine of approximately every individual to check their profile every day as recognized by Michael Fire et al. [1]. Although it comprises a vast number of clients and it a hub of data, this has become a feasible path for attackers to use or assault. Many websites offers diverse things to prevent these sorts of assaults but it is complicated to end them because they have a variety of fresh methods each day to performing assault. Due to the user friendly environment of Facebook, users are expected to reveal many private information about themselves and their links as offered by Abu-Nimeh et al. [2].

The information may contain date of birth, private pictures, place of service, email address, high school name, relationship status, and even mobile number. If this private data is taken by hateful user then it is to them to carry out malicious actions on their timeline or even in their private life [3]. For example, a hateful user can utilize the private data taken from the Facebook website to send customized

spam posts to user. In Facebook there are various third party requests accessed by the web user. When user wants to drive any third party request then user must permit the authorization to access the some profiles information by the application. When user permits the authorization then application can see the user's private information like name, email id and friends list etc. Occasionally hackers generate these applications and influence the user to utilize these hateful Apps. Customer accesses malicious Apps and has to share its private details with App. Hacker takes benefit of user's private details and posts hateful stuff on user's wall.

Amongst the diverse examination relating to Twitter, spam accounts recognition is one of the mainly considered and applicable one. In universal terms, spammers are beings, real users or mechanical bots, whose intend is to frequently distribute messages that include useless content for profitable functions [13], links to hateful websites, in order to extend malwares, phishing attacks, and other damaging action [5].

II. RELATED WORK

Daya L. Mevada [6] prescribed strategies to find opinion spam from large measure of unstructured records has become a critical exploration trouble. This examination prompts a sentiment spam analyzer which over and again sort input text data into either spam or non-spam gathering. The arranged framework will apply artificial intelligence directed strategy.

M.N. Istiaq et. al. [7] authors has present a article which finds the chance of starting dynamic learning for

recognizing Review spams performed on genuine records which exhibits promising results. All through the methodology, they qualified model using dynamic taking in procedure which gains from the most phenomenal models in various emphases.

Rashmi Gomatesh et. Al. [9] anticipated their perception in the article "Recognition of Fake Review and Brand Spam Using Data Mining Technique". This strategy proposed a conduct way to deal with spot audit spammers the individuals who are attempting to control the evaluations on hardly any things. Author determines a joined activity methods for grade analysts dependent fair and square that they have checked the spamming practices. They affirmed anticipated methods by performing client estimation on an Amazon dataset which holds surveys of various organization's things.

SP.Rajamohana, et. al. [10] Focused light on misdirecting surveys that are effectively open in the web which slowly more influences organizations and customers. Along these lines it is critical to notice and expel such bogus feeds from online locales. This record uncovers a few methodologies used for audit spam acknowledgment and execution measures were perceived.

Mubarak et al. [11] introduced an effortless methods for understanding the hypothesis. People may like to channel information for various reasons, for example, the need of ordering information, kill obscene substance from the media stream, or prevent kids from seeing unambiguous posted messages. Every one of these targets manual for component learning interchanges with the Twitter API and different limits. A further inside and out assessment of spamming hurts reveals building calculations, for example, NB IBK (which is may allude to Ibk calculation, applies the k-NN calculation) as methods for finding answers for the trouble.

Ameen and Kaya [12] proposed out a related work and found that easygoing backwoods had the greatest accomplishment at 92.95%. An examiner must research to discover the best calculation to use before going with further examination. There is no fastidious calculation that goes past all others under all conditions; this explains the need of exploration with various methodologies. Prior to moving towards higher classifier techniques, it is important to value the reason that most of analysts have release SVM classifiers, for example, sack of-words and pack of-implies.

Alshehri et al. [13] use hashtags and N-grams to show out grown-up Arabic substance. The pack of-words procedure uses twofold qualities to guarantee for positive words in a posted substance, while sack of-implies include discovering a normal of word vectors. The result of their inspect was a 79% precision of preparing.

III. PROPOSED METHODOLOGY

In this section proposed bot detection model was explained where working steps were explained by block diagram shown in fig. 1. Each block was detail in below subsection.

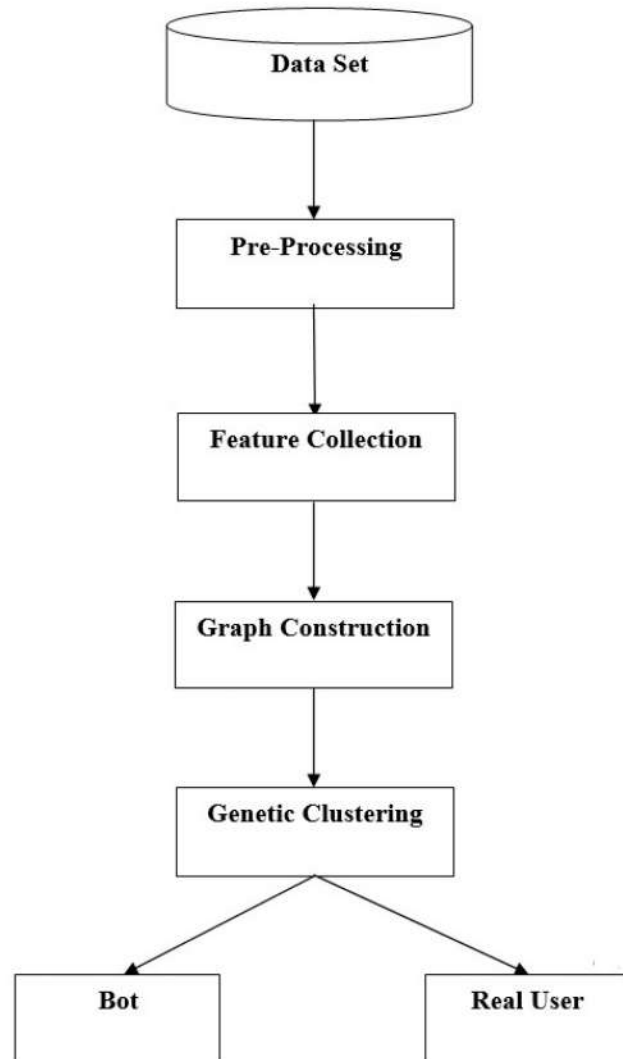


Fig. 1 Proposed work Block diagram.

1. Pre-processing

Preprocessing is a procedure utilized for transformation of content into feature vector. Much the same as content orders the preprocessing additionally has debate about its division.

This work uses tweets preprocessing which comprise of words in charge of bringing down the execution of learning models. Here dataset contain some of columns which are not fruitful for this work, hence those information is either delete or transform into different state. Information preprocessing diminishes the extent of the info content records fundamentally. It includes exercises like sentence

limit assurance, common language particular stop word disposal and stemming.

2. Feature collection

This work twitter dataset was consider as the input where nine features of each user were extract. These features F represent the user behavior on the social network. Table 1 shows feature set utilize in this work.

- Sequence of Shares
- Sequence of Likes instance
- Sequence of Tweets perform by user
- Sequence of re-tweet perform by user
- Time instance of the event

Feature from 1 to 5 can be easily extract from the dataset where as per the behavior follow by the user.

3. Transition probability between action events steams

$P(i,j)$ represents the probability that the click action is j at timestamp t followed by click action at timesptamp $t-1$. So probability find the relation between the i and j features of the use in form of transition done in a specific set of durations.

$$P(i,j) = \frac{\sum_1^t X_i \rightarrow X_j}{\sum_1^t X_i}$$

In above equation $X_i \rightarrow X_j$ act as transition form i to j feature instance, while t as the total time instance when i feature were applied. So if work use n number of features than each user has a feature vector of $n \times n$ where cell contain a probability transition value.

$$F_x = \begin{vmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{vmatrix}$$

4. Graph Construction

In this step develop a completely connected graph where each node is connect with other node and distance between them act as weight of the edge. Estimation of the distance was done by using X and Y axis of the system. Here this can be understand as let nodes are $N = \{n1, n2, n3, \dots, nm\}$ and distance between them are evaluate by Euclidian distance formula.

Now sort graph edges with Minimum Weight in a decreasing order. This can be understand as matrix $S[]$ of

three column and rows depend on number of edges present in the graph.

5. Resultant cluster

So nodes which are present with less distance edge weights are considered as the true user or real user of the social media. While nodes whose distance values are larger in oter cluster were consider as the bots. As each bot set of instance sequence were totally different from real user set of instances, so distance from other existing nodes were high. Hence cluster selection of real or bot is depends on the weight value of the partial tree present in the cluster.

6. Generate Population

Here assume some cluster centers from the graph node. This is generate by the random function which select fix number of image cluster for the centroid. This can be understand as let the number of centroid be C_n , then one of the possible solution is $\{C1, C2, \dots, Cn\}$. In the similar fashion other possible solutions are prepared which can be utilize for creating initial population matrix.

7. Fitness Function

For finding difference between users Fitness function similarity was used for evaluating the similarity between the profile, content and self mention. Sort the similarity matrix in descending order to assign the user to the centroid. As each feature give its separate index to the population of the genetic algorithm so different weight assign for each feature.

8. Teacher Phase

Top possible solution after sorting will act as the teacher for other possible solutions. Now selected teacher will teach other possible solution by replacing fix number of centroid as present in teacher solution. By this all possible solution which act as student will learn from best solution which act as teacher. Here each possible solution is evaluated for finding the distance from each centroid so that user closer to the centroid are cluster together. Then calculate the fitness value which give overall rank of the possible solution.

Main motive of this step is to find best solution from the generated population. This difference modifies the existing solution according to the following expression

$$X_{new,i} = \text{Difference}(X_{teacher,i}, X_{student,i})$$

Where $X_{new,i}$ is the updated value of $X_{student,i}$. Accept $X_{teacher, i}$ value.

9. Student Phase

In this phase all possible solution after teacher phase are group for self learning from each other. This can be understand as let group contain two student then each student who is best as compare to other will teach other solution. Teaching is similar as done in teacher phase, here replacing fix number of centroid is done which is similar as in best student of the group.

Once student phase is over then check for the maximum iteration for the teaching if iteration not reach to the maximum value then GOTO step of teacher phase else stop learning and the best solution from the available population is consider as the final centroid of the work. Now image are cluster as per centroid.

10. Final Solution

In this work after sufficient number of iteration cluster centers are obtained and assign users to those clusters. Here each cluster is represent by its cluster center. So as per the different number of user type available in the dataset number of clusters are generate.

IV. EXPERIMENTAL SETUP

Whole work was implement on MATLAB software. It is utilize on account of its rich library which has numerous inbuilt storage that can be specifically use in this work for various reason. Out of various storage few are crossing point, contrasting of the string, and so forth. One more essential factor is its GUI by which one who doesn't know about the code can straightforwardly runs the storage without having earlier information.

1. Dataset

In this work experiment is done on social dataset content obtained from <https://botometer.iuni.iu.edu/bot-repository/datasets.html>, where as per the user related twitter comments of respected user with different action and timestamp were available. Description of the dataset is available in table 1.

Table 1 Experimental dataset detailed description.

Features	Values
Instances	36462
Users	29
Data Year	1
Actions	4

2. Results

Results of proposed model was compared with previous work proposed in [14].

Table 2 Accuracy Based Comparison.

Data Size	Proposed Work	Previous Work
28000	0.7931	0.5652
35000	0.7931	0.6552
42000	0.7667	0.6333
49000	0.7667	0.6333

28000	0.7931	0.5652
35000	0.7931	0.6552
42000	0.7667	0.6333
49000	0.7667	0.6333

Above table 2 has shown that proposed model has increase the bot detection accuracy of work. Feature selection has increase the graph clustering algorithm accuracy. Further paper has involve the genetic algorithm which give user features as per class.

Table 3 Precision Based Comparison.

Data Size	Proposed Work	Previous Work
28000	1	0.7647
35000	1	0.8261
42000	1	0.8261
49000	1	0.8261

Above table 3 has shown that proposed model has increase the classification accuracy of work. Values shows that use of graph clustering algorithm has reduce the confusion of user identity. Further paper has involve the genetic algorithm which give user features as per class.

Table 4 Recall Based Comparison.

Data Size	Proposed Work	Previous Work
28000	0.7391	0.6842
35000	0.7931	0.76
42000	0.7667	0.7308
49000	0.7667	0.7308

Above table 4 has shown that proposed model has increase the classification accuracy of work. Values shows that use of graph clustering algorithm has reduce the confusion of user identity. Further paper has involve the genetic algorithm which give user features as per class.

Table 5 F-measure Based Comparison.

Data Size	Proposed Work	Previous Work
28000	0.85	0.7222
35000	0.8846	0.7917
42000	0.8679	0.7755
49000	0.8679	0.7755

Above table 2 has shown that proposed model has increase the bot detection accuracy of work. Feature selection has increase the graph clustering algorithm accuracy. Further paper has involve the genetic algorithm which give user features as per class.

V. CONCLUSIONS

Life of social media depends on real user action but digital user perform unfair action and reduce overall trust value. Many of social site execute bot detection algorithm. This

paper has proposed a graph based genetic algorithm for bot detection. Input of this algorithm was set of user action and based on these action transition probability features user were cluster into two class. Output of graph based clustering algorithm were pass into genetic algorithm. TLBO algorithm finds the bot user feature set and real user feature set. Experiment was perform on twitter real dataset and results shows that proposed model has increase the bot detection accuracy by 11.68%. In future researcher can perform bot detection by using artificial intelligence method.

REFERENCES

- [1] Morris, M. and Ogan, C. (1996). The internet as mass medium. *Journal of communication*, 46(1):39-50.
- [2] Lee, K., Eo, B. D., and Caverlee, J. (2011). Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter. In *Proc. AAAI Intl. Conf. on Web and Social Media (ICWSM)*.
- [3] Ferrara, E., Varol, O., Davis, C., Menczer, F., and Flammini, A. (2016a). The rise of social bots. *Communications of the ACM*, 59(7):96-104.
- [4] Jun, Y., Meng, R., and Johar, G. V. (2017). Perceived social presence reduces fact-checking. *Proceedings of the National Academy of Sciences*, 114(23):5976-5981.
- [5] Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10):94-100.
- [6] Mevada D. L., Daxini V., "An opinion spam analyzer for product Reviews using supervised machine Learning method." pp.03, (2015).
- [7] M. N. Istiaq Ahsan, Tamzid Nahian, Abdullah All Kafi, Md. Ismail Hossain, Faisal Muhammad Shah "Review Spam Detection using Active Learning." 978-1-5090-0996-1, pp.16, (2016).
- [8] Michael C., et al. "Survey of review spam detection using machine learning techniques." *Journal of Big Data* 2.1, pp.9, (2015).
- [9] Adike R. G., Reddy V., "Detection of Fake Review and Brand Spam Using Data Mining Technique.", pp.02, (2016).
- [10] Rajamohana S. P, Umamaheswari K., Dharani M., Vedackshya R., "Survey of review spam detection using machine learning techniques." 978-1-50905778-8, pp.17 (2017).
- [11] Mubarak, H.; Darwish, K.; Magdy, W. Abusive language detection on Arabic social media. In *Proceedings of the First Workshop on Abusive Language Online*, Vancouver, BC, Canada, 4-7 August 2017; pp. 52-56.
- [12] Ameen, A.K.; Kaya, B. Detecting spammers in twitter network. *Int. J. Appl. Math. Electron. Comput.* 2017, 5, 71-75.
- [13] Alshehri, A.; Nagoudi, A.; Hassan, A.; Abdul-Mageed, M. Think before your click: Data and models for adult content in arabic twitter. In *Proceedings of the 2nd Text Analytics for Cybersecurity and Online Safety (TA-COS-2018)*, 2018.
- [14] Peining Shi, Zhiyong Zhang And Kim-Kwang Raymond Choo. "Detecting Malicious Social Bots Based on clickstream Sequences". *IEEE Access* March 18, 2019.