International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Graph Based Digital Spammer Identification by User Click Behavior

Rupali Vishwakarma, Pratima Gautam

Abstract*: As social media network popularity increases day by day, content writer are spamming on these platform for potential benefits of some organizations. Some of blogs are fabricate which invite users to external phishing sites or malware downloads huge security issue online and undermined the user experience. This work has proposed an un-supervised technique for identifying the real users from the social network spammers. Here graph based clustering algorithm was proposed to develop a binary cluster on the basis of serial or sequential action perform by the user. As per series of action social network graph is reduce into spanning tree where highly distance nodes are identified as abnormal behavior. So group of highly distance nodes are consider as the social spammers while other are real users. Experiment was perform on real social sequential dataset of twitter. Results were compared on various evaluation parameters and it was obtained that proposed approach has improved all such parameter values as compared to previous approach adopt by researcher.

Keywords: Online Social Networks (OSNs), Twitter, Spammers, Legitimate users.

I. INTRODUCTION

During the previous two decades, people logically gone to the Internet and online life to discover news, share emotions and engage in discussions [1]. So knowledge obtained from this source has great impacts on all parts of our everyday lives, including our political, wellbeing, money related, and family choices. This expanded impact of web based life has been joined by an expansion in events to change the natural idea of our online talks and sharing of thoughts. Specifically, in the course of recent years people have seen a explosion of social spammers [2], a nearness that doesn't give indications of decay in social digital platform. Social spammers are internet based life records controlled totally or to a limited extent by algorithms. They can create content naturally and collaborate with human users, regularly acting like, or copying, people [3].

So this paper, focus on those live characters r users in online informal communities that clandestinely expect to control open talk and impact human feelings and behave in a unclear manner. While progressively conventional wicked elements, as malware, assault vulnerabilities of equipment and programming, social spammers misuse human vulnerabilities, for example, our inclinations to focus on what gives off an impression of being mainstream and to confide in social contacts (Jun et al., 2017)[4]. Spammers develop more than one account where they can rapidly produce posts and make explicit substance pattern or enhance wrong information. Spammers can deceive people and commitment based positioning calculations alike, making the appearance that some individual or thought is prevalent.

In this way, protecting from social spammers raises genuine research difficulties [5]. Misleading population thought isn't new; it has been a typical practice since the beginning of mankind. The innovative apparatuses like printed media, radio, TV, and the Internet — have been manhandled to scatter deception and publicity. The tricky procedures utilized on every one of these sorts of channels offer striking similarity [6]. In any case, internet based life are especially defenseless in light of the fact that they encourage programmed associations by means of programming. Thus, online networking stages need to battle a downpour of attacks. Facebook as of late reported that 1.5 billion spammer records were evacuated more than a half year in 2018. Even a low miss rate could leave a large number of records accessible to be utilized as spammers. In this light, it isn't amazing that upwards of 9–15% of dynamic Twitter records were assessed to be spammers in 2017 [7], and that social spammers are in charge of producing 66% of connections to famous sites [8]. Open enthusiasm for social spammers has additionally significantly expanded during the previous couple of years.

II. RELATED WORK

McCord et.al. [9] utilized user based features like number of following, number of likes and content based features like number of URLs, answers/makes reference to, retweets, hashtags of gathered database. Classifiers to be specific Random Forest, Support Vector Machine (SVM), Naive Bayesian and K-Nearest Neighbor have been utilized to distinguish spam profiles in Twitter. Restriction of this methodology is that for considered dataset notoriety highlight has been indicating incorrectly results for example it can't separate spammers and non-spammers, lopsided dataset has been utilized so Random Forest is giving best outcomes as this classifier is commonly utilized if there should be an occurrence of uneven dataset, lastly the methodology has been approved on less dataset.

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author
Rupali Vishwakarma*, Phd Scholar, Department of Computer Science &Engineering, AISECT University Bhopal, MP, India. Email: xyz1@blueeyesintlligence.org
Dr. Pratima Gautam, Department of Computer Science & Engineering, AISECT University Bhopal, MP, India.. Email: pratima_shkl@yahoo.com

Lee et. al.[10] sent social honeypots comprising of real profiles that distinguished suspicious users and its bot gathered proof of the spam by creeping the profile of the user sending the undesirable companion solicitations and hyperlinks in MySpace and Twitter. Features of profiles like their posting conduct, substance and companion data to build up an AI classifier have been utilized for distinguishing spammers.

After investigation profiles of users who sent spontaneous companion solicitations to these social honeypots in MySpace and Twitter have been gathered.

LIBSVM classifier has been utilized for distinguishing proof of spammers. Constraint of the methodology is that less dataset has been utilized for approval.

Benevenuto et. al. [14] recognized spammers based on tweet substance and user based features. Tweet substance qualities utilized are - number of hashtags per number of words in each tweet, number of URLs per word, number of expressions of each tweet, number of characters of each tweet, number of URLs in each tweet, number of hashtags in each tweet, number of numeric characters that show up in the content, number of users referenced in each tweet, number of times the tweet has been retweeted. Portion of tweets containing URLs, division of tweets that contains spam words, and normal number of words that are hashtags on the tweets are the qualities that separate spammers from non spammers.

Gee et. al. [15] utilized this feature and detected spam profiles using classification technique. Normal user profiles have been collected using Twitter API and spam profiles have been collected from "@spam" in Twitter. Collected data was represented in JSON then it was presented in matrix form using CSV format. Matrix has users as rows and features as columns. Then CSV files were trained using Naive Bayes algorithm with 27% error rate then SVM algorithm has been used with error rate of 10%. Spam profiles detection accuracy is 89.3%. Limitation of this approach is that not very technical features have been used for detection and precision is also less i.e. 89.3% so it has been suggested that aggressive deployment of any system should be done only if precision is more than 99%.

Yang et al. [16] collect Sybil accounts from Renren as ground-truth data set. Then, they analyse it by using network-based and structured-based features such as network clustering coefficient, incoming and outgoing request rate.

III. PROPOSED METHODOLOGY

In this work the social user behavior and sorts the spammers in the cluster without having any earlier information of the individual tweet / comment. In the propose work no need of any configuration for the information, for example, speakers recognizable proof image or exceptional character, here all procedure is finished by using the diverse techniques of content mining.

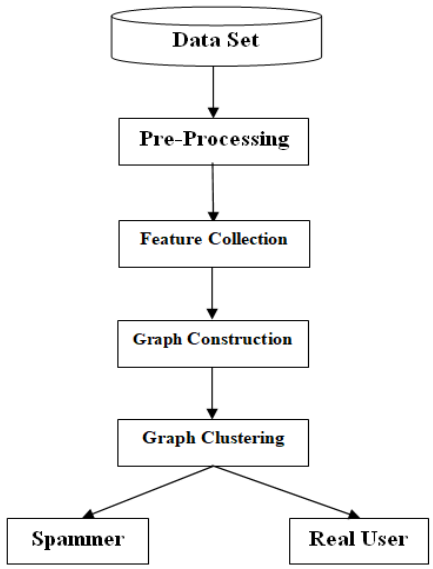

Fig.1. Block diagram of proposed graph based Spammer detection.

A. Pre-Processing

such that As the dataset is a collection of data which is unorganized and need to retrieve important information which is fruitful for the work in this work dataset contain time, date, protocol, session, etc. Here data is clean and transform this as per working environment. Preprocessing is a procedure utilized for transformation of content into feature vector. Here Stop-words are functional words which happen as often as possible in the language of the content (for instance a, the, an, of and so forth in English language), with the goal that they are not valuable for characterization. Here work read entire task and put all words in the vector.

B. Feature Collection

In 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.

Table- II: Name of the Table that justify the values

1	Total number of Has tag
2	Total number of URLS used by user
3	Average number of URLs in a tweet
4	Average number of URLs/words in a tweet
5	Average number of hashtags/words in a tweet
6	Total number of words
7	Total tweets
8	User's tweets that contain the URLs/Tweet
9	User Inter content relation

Feature from 1 to 8 can be easily extract from the user tweet but the last or 9th feature need some more steps like pre-processing followed by relation evaluation.

C. 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 = {n_1, n_2, n_3,……..n_m} and distance between them are evaluate by Euclidian distance formula.

$$DD^{f}_{x,y} = \sqrt{(XX_{f11} - YX_{f11})^2 + (XX_{f12} - YX_{f12})^2 \ldots\ldots\ldots\ldots + (XX_{fnn} - YX_{fnn})^2}$$

Where X and Y are feature values of ending nodes, while $XX_{f12}$is the X user feature of action event 1and action event 2.

Now sort graph edges with Minimum Weight in a decreasing order. This can be understand as matrix of three column and rows depend on number of edges present in the graph. Let a shorted matrix of S=6X3 was developed in this step. Table 2 shows this sorted matrix.

Node	Node	Weight
2	4	2
4	1	4
5	3	4
6	5	7
5	4	14
5	3	18

D. Minimum Spanning Tree

In this step above S[] act as input where first row or first edge with minimum weight was select in spanning tree construction. Mark each of these node as CHK. Now for each new row of S[] check that either of vertex or node present in the CHK matrix. If both the vertex of new row are already present in the matrix than ignore this row, other wise include new vertex and mark them as CHK.

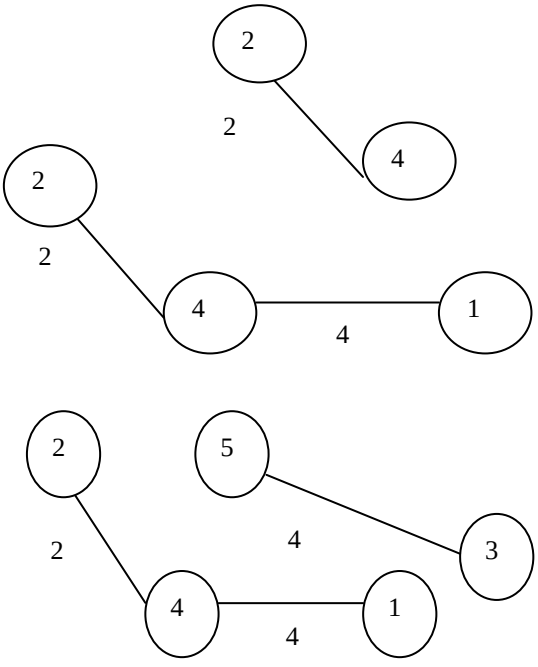

Fig.2. Graphical representation of spanning tree construction where nodes are user and weights are there feature relation.

This work use Kruskal's algorithm for tree construction whereas per edge present in table 2 sortest weight edge was considered. Fig. 2 a shows first row of the tree while fig. 4.3 b shows second row insertion in tree. In similar way other set of nodes were include in the trees. Each new row insertion involve at-least one new node in the tree.

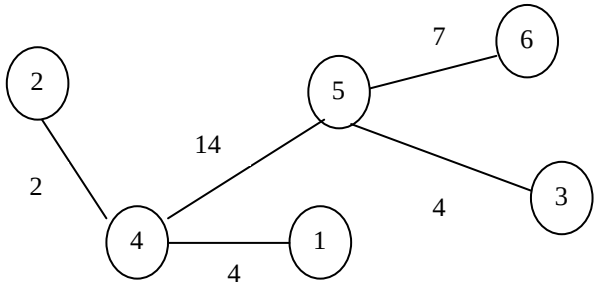

Fig.3. Spanning Tree of table 2 graph.

Fig.3. shows final spanning tree of the table 2. Here all set of six nodes present in table 2 were connected by edges while overall weight of the tree was also minimum. Hence nodes which have higher distance from other node get easily separated without any training.

E. Graph Clustering

Once minimum spanning tree obtain than remove highly weighted edges of the tree such that whole tree get break into K cluster. This can be understand as

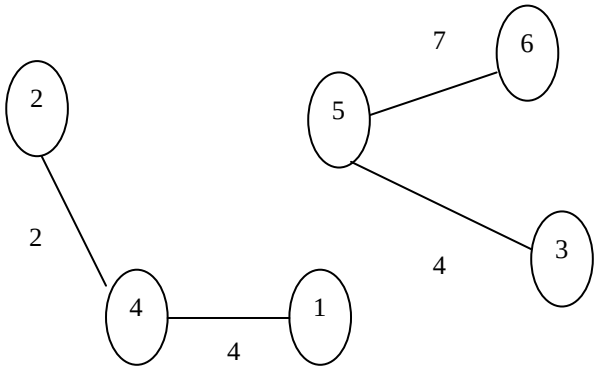

Fig.4. Clustered Spanning Tree of table 1 graph.

Figure 4: shows that by removing highly weighted edge one can obtain clusters of node which are closer to each other as per distance. Here it was also obtained that proposed clustering algorithm can easily generate k clusters by simply removing the highly weighted edge only. This algorithm not required any iteration or other thing.

F. 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 other cluster were consider as the spammers. As each spammer 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 spammer is depends on the weight value of the partial tree present in the cluster

Proposed Algorithm\

Input: DS // DS: Dataset

Ouput: C_r C_b// C_r: Cluster of real user, C_b : Cluster of social Spammer

1. PD←Pre-Processing(DS)
2. Loop 1:n// n: number of users
3. Loop 1:i // i, j: User Features
4. F(i,j)←Feature(PD,n,i)
5. EndLoop
6. EndLoop
7. FCG←Fully_connected_graph(F, n)// FCG: Fully Connected Graph
8. ST←Spanning_Tree(FCG)
9. Loop 1:n
10. If W(ST,n) > T
11. C_r←n
12. Otherwise
13. C_b←n
14. EndIf
15. EndLoop

IV. EVALUATION PARAMETERS

If you are using *Word*, use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). "Float over text" should *not* be selected.

A. Precision: Precision value is the ratio of predicted positive user to the totalpredicted user.

$$Precision = \left(\frac{True_{positive}}{(False_{positive} + True_{positive})}\right)$$

B. Recall: The recall is the fraction of relevant users that have been predicted over the total amount of input users. It is also known as Sensitivity or Completeness.

$$Recall = \left(\frac{True_{positive}}{False_{negative} + True_{positive}}\right)$$

C. F-Measure: Harmonic mean of precision value and recall value is F-measure.

$$F - Measure = \left(\frac{2xPrecisionxRecall}{(Recall + Precision)}\right)$$

D. Accuracy: This act as the percentage of correct prediction from the total set of prediction.

$$Accuracy = \left(\frac{Correct\_class}{(Correct\_class + InCorrect\_class)}\right)$$

E. Dataset

In this work twitter dataset named as twitter_cikm_2010 [] was used which have three column first was USER-ID, Twitter-ID and Tweet. For testing 1057 tweets were used for the classification of user into Real or Fake class.

F. Results

Results of the proposed work **GBSD** (Graph Based Spammer Detection) is compare with the existing method in HITS [10].

Table II: Precision value comparison of GBSD and HITS work.

Dataset	HITS	GBSD
18	0.6	0.9
24	0.5385	0.7692
27	0.6667	0.6667

Table 2 shows that Precision value of proposed GBSD was high as compared to previous algorithm HITS. Here proper leaning feature with pre-processing filter increase the efficiency of the work. It has been observed that proposed work content feature selection plays an important role for unsupervised classification of data into blogger and spammers.

Table III: Recall value comparison of proposed and previous.

Dataset	HITS	FCMRF
18	0.7500	1
24	0.6364	0.9091
27	0.7143	0.8333

Above table 3 shows that Recall value of proposed work was high as compared to previous algorithm HITS. Here proper weight assignment of edges as per features values gives better result. It was obtained that user content relation building increase the efficiency of work as it directly identify the similarity between user content.

Table IV: F-Measure value comparison of proposed and previous work.

Dataset	HITS	GBSD
18	0.6667	0.9474
24	0.5833	0.8333
27	0.6897	0.7407

Above table 4 shows that F-Measure value of proposed GBSD was high as compared to previous algorithm HITS. Here proper leaning feature with pre-processing filter increase the efficiency of the work. It has been observed that proposed work content feature selection plays an important role for unsupervised classification of data into blogger and spammers.

Table V: Accuracy value comparison of proposed and previous work.

Dataset	HITS	GBSD
18	0.6667	0.9444
24	0.5833	0.8333
27	0.6667	0.7407

Above table 5 shows that Precision value of proposed GBSD was high as compared to previous algorithm HITS. Here proper weight assignment of edges as per features values gives better result. It was obtained that user content relation building increase the efficiency of work as it directly identifies the similarity between user content.

V.CONCLUSIONS

Social network is place to connect and share thoughts with each other. But most of people get attract from the social audience gathering for there personal or professional advantages. In the propose work no need of any configuration for the information, for example, speakers recognizable proof image or exceptional character. This work presents a study of methods for detection of user profiles as real or social spammer. Here a technique GBSD was proposed for classifying the social nodes into two cluster, where digital social network graph was reduce into spanning tree. Here weight of the graph was social sequential action transitional probability. So each node has its own set of transitional probability and distance between nodes of transitional probability act as weight of graph. So as per graph clustering technique spanning tree was developed and highly weighed nodes of this tree act as social spammer cluster while other set of nodes are real. Results shows that proposed graph based clustering technique has increase the precision value as compared to previous approach used in [12]. While recall value was also increase, at the same time accuracy of the social spammer identification was also increase.

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 re-duces 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. Boshmaf, Y., Muslukhov, I., Beznosov, K., and Ripeanu, M. (2012). Key chal- lenges in defending against malicious socialbots. In Proc. 5th USENIX Conference on Large-Scale Exploits and Emergent Threats (LEET).
7. Varol, O. and Uluturk, I. (2018). Deception strategies and threats for online discussions. First Monday, 22(5).
8. Wojcik, S., Messing, S., Smith, A., Rainie, L., and Hitlin, P. (2018). Bots in the twittersphere. Pew Research Center, Washington, D.C.
9. M. McCord, M. Chuah, Spam Detection on Twitter Using Traditional Classifiers, ATC'11, Banff, Canada, Sept 2-4, 2011, IEEE.
10. Kyumin Lee, James Caverlee, Steve Webb, Uncovering Social Spammers: Social Honeypots + Machine Learning, Proceeding of the 33rd international ACM SIGIR conference on Research and development in information retrieval, 2010, Pages 435–442, ACM, New York (2010).
11. Hua SHEN,Xinyue LIU. "Detecting Spammers on Twitter Based on Content and Social Interaction", International Conference on Network and Information Systems for Computers, 2015.
12. Muhammad U. S. Khan, Member, Mazhar Ali, Member, Assad Abbas, Student Member, Samee U. Khan, Senior Member and Albert Y. Zomaya. "Segregating Spammers and Unsolicited Bloggers from Genuine Experts on Twitter". IEEE Computer Society 2016.
13. 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, pp. 811-824, 2012.
14. Fabricio Benevenuto, Gabriel Magno, Tiago Rodrigues, and Virgilio Almeida, Detecting Spammers on Twitter, CEAS 2010 Seventh annual Collaboration, Electronic messaging, Anti Abuse and Spam Conference, July 2010, Washington, US
15. Grace gee, Hakson Teh, Twitter Spammer Profile Detection, 2010.
16. Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering social network sybils in the wild," ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 8, p. 2, 2014.
17. M. A. Rajab, J. Zarfoss, F. Monrose and A. Terzis,\ A multifaceted approach to understanding the bot-
18. 18. Net phenomenon," in Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement (IMC'06), pp. 41-52, 2006. achievements, with photo that will be maximum 200-400 words.