Current Trends in Technology and Science
www.ctts.in, ISSN: 2279-0535, May-2021, Volume: X, Issue: III

Survey on Digital Platform Malicious Bot Detection Techniques and Features

Kamlesh Kori [1], Rajesh Ku. Nigam [2], Dr. Bhupendra Verma [3]

[1] Research Scholar, CSE Department., Technocrats Institute of Technology & Science, Bhopal (India) (kamleshkori45@gmail.com)
[2]Associate Professor, CSE Department., Technocrats Institute of Technology, Bhopal (India) (rajeshrewa37@gmail.com)
[3] Professor, CSE Department., Technocrats Institute of Technology, Bhopal (India) (bkverma3@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 a bot. Several researchers have proposed different techniques to identify these bots, which was a post by bot programs. The paper has briefed some of the techniques proposed by the researcher to differentiate human and machine behaviour on social sites. Social site features set also listed in the paper directly or indirectly identify the artificial user (BOT). Recent researcher methodologies were also summarized in this paper.*

Index Terms— Data mining, Online Social Networks, Spammers, BOT Detection.

INTRODUCTION

By using the Internet, it has become quite natural to receive any information from any source worldwide. The increased demand from social sites allows users to gather an abundance of user information and data. Enormous amounts of data on these pages often draw the attention of fake users [1]. Twitter has rapidly become an online source for acquiring real-time information about users. Twitter is an Online Social Network (OSN) where users can share anything and everything, such as news, opinions, and even their moods. Several arguments can be held over different topics, such as politics, current affairs, and important events. When a user tweets something, it is instantly conveyed to their followers, allowing them to outspread the received information at a much broader level [2]. With the evolution of OSNs, the need to study and analyze users' behaviours in online social platforms has intensity. The fraudsters can easily trick many people who do not have much information regarding the OSNs. There is also a demand to combat and control the people who use OSNs only for advertisements and thus bot other people's accounts. Recently, the detection of the robot (BOT) in social networking sites attracted the attention of researchers. BOT detection is a difficult task in maintaining the security of social networks. It is essential to recognize bots in the OSN sites to save users from various malicious attacks and preserve their security and privacy. These hazardous manoeuvres adopted by bots cause massive destruction of the community in the real world. Twitter bots have various objectives, such as spreading invalid information, fake news, rumours, and spontaneous messages. Bots achieve their malicious objectives through advertisements and several other means where they support different mailing lists and subsequently dispatch bot messages randomly to broadcast their interests. These activities cause disturbance to the original users, who are known as non-bots. In addition, it also decreases the repute of the OSN platforms. Several research works have been carried out in the domain of Twitter bot detection. A few surveys have also been carried out on fake user identification from Twitter to encompass the existing state-of-the-art. Tingmin et al. [4] provide a survey of new methods and techniques to identify Twitter spam detection. The above survey presents a comparative study of the current approaches.

On the other hand, the authors in [5] surveyed different behaviours exhibited by bot/spammer on a Twitter social network. The study also provides a literature review that recognizes the existence of spammer on the Twitter social network. Despite all the existing studies, there is still a gap in the existing literature. Therefore, we review the state-of-the-art bot detection and fake user identification on Twitter to bridge the gap. Moreover, this survey presents a taxonomy of the Twitter bot detection approaches and attempts to offer a detailed description of recent developments in the domain.

RELATED WORK

Ameen and Kaya [6] proposed 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 to explore various methodologies. Before moving towards higher classifier techniques, it is important to value why most analysts have released SVM classifiers, such as a sack of words and a pack of implies.

Lee et. al.[7] deployed social honeypots consisting of genuine profiles that detected suspicious users, and its bot collected evidence of the spam by crawling the user's profile sending the unwanted friend requests and hyperlinks in MySpace and Twitter. Features of profiles like their posting behaviour, content and friend information to develop a machine learning classifier have been used for identifying spammers. After analysis, profiles of users who sent unsolicited friend requests to these social honeypots in MySpace and Twitter have been collected. LIBSVM classifier has been used for the identification of spammers. One good point in the approach is that it has been validated on two different dataset combinations – once with 10% spammers+90% non-spammers and 10% non-spammers+90% spammers. The limitation of the approach is that less dataset has been used for validation.

Viswanath et al. [8] discover that dependency on community detection makes more vulnerable to Sybil attacks where honest identities conform to strong communities. Because Sybils can infiltrate honest communities by carefully targeting honest accounts, that is, Sybils can be hidden as just another community on OSN by setting up a small number of the targeted links. The targeted links are the links given to the community which contains the trusted node. They make an experiment by allowing Sybils to place their links closer to the trusted node instead of random nodes, where closeness is defined by ranking used by the community detection algorithm they employ. Hence, Sybil nodes are high ranked in the defence scheme. Naturally, it leads to Sybils being less likely to be detected for that attack model because Sybils appear as part of the local community of the trusted node.

Boshmaf et al. [9] point out that structure-based Sybil detection algorithms should be designed to find local community structures around known honest (non-Sybil) identities while incrementally tracking changes in the network by adding or deleting some nodes and edges dynamically in some period for better detection performance.

Alshehri et al. [10] use hashtags and N-grams to show out grown-up Arabic substance. The pack of words procedure uses twofold qualities to guarantee positive words in a posted substance, while a sack of implies includes discovering a normal of word vectors. The result of their inspection was a 79% precision of preparation.

Peining Shi et al. in [11] novel method of detecting malicious social bots, including both features selection based on the transition probability of clickstream sequences and semi-supervised clustering, is presented in this paper. This method analyzes the transition probability of user behaviour clickstreams and considers the time feature of behaviour.

Techniques of Bot Detection

Traffic-based Detection:- The P2P bots speak with numerous other friend bots to get or receive instructions, send collected data and get new instruction or work, in this manner persistently creating enormous traffic [12, 13]. Different traffic-based detection methods have been proposed, which inspect the system traffic and centre to watch the traffic patterns.

Behaviour-based Detection:- A thorough investigation of botnet estimations by Rajab et al. [14] uncovers botnets' basic and social properties. Bots may likewise have numerous inner characteristics, keep up the permanent associations with other companion bots and get the orders from botmaster through servers. It is seen that the system conduct qualities of P2P botnets are attached to the basic engineering and action instruments.

DNS-based Detection:-The bots have a collective action as a key component and, as often as possible, use DNS to rally servers, dispatch content (noise) and update their codes. Bots of the same botnet contact a similar space, occasionally prompting comparable DNS traffic, different from genuine clients [15].

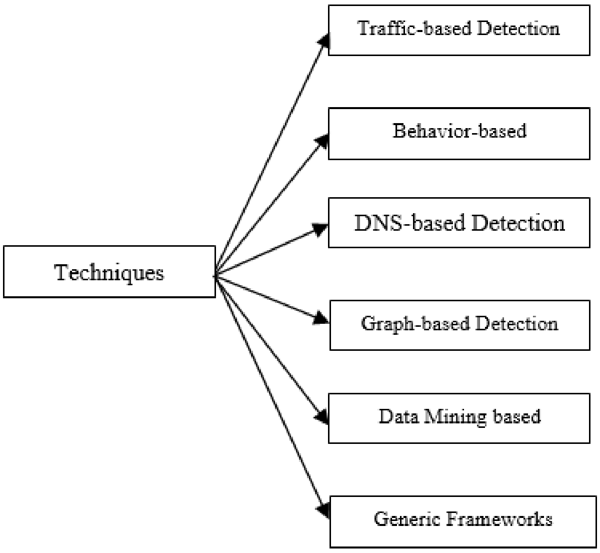

Figure 1 Different techniques of social bot detection.

Graph-based Detection:- The graphical structure is an inherent feature of the botnets and is useful to understand how botnets communicate internally. The graphical analysis of the botnet communication network can be used to find the characteristic patterns of the botnets. The P2P C&C communications graph exhibit the topological features useful for traffic classification and botnet detection.

Data Mining-based Detection:- The data mining techniques can be used to detect an anomaly, i.e., unusual or fraudulent behaviour. Data mining techniques are used for malicious code detection and intrusion detection. Many authors have used classification and clustering techniques to detect botnet C&C traffic efficiently.

Generic Frameworks:- Some general botnet detection frameworks have been proposed based on behaviour monitoring and traffic correlation analysis. Bot Miner is a general framework for botnet detection [10]. The system detects botnets based on network packets and flows analysis. It relies on behaviour monitoring and traffic correlation analysis, mostly applicable at a small scale and does not scale well because it requires analysis of vast amounts of fine-grained information.

Feature Extraction

Social bot detection is based on classifications of selected features to sort accounts into either legitimate or bot accounts. However, the studies reviewed in this paper highlight how common features are used to detect social bot accounts. These include factors related to timing, automation, text use, sentiment, and clickstream behaviour. Therefore, we cannot assume a social bot depends on one feature without addressing the other features [15]. Table I summarises the common features extracted from a full set of features in the reviewed papers to measure whether an account is a human or bot. In general, the extracted features can address the network features to identify the community features. We can also identify the social connections of users and ranking through performing content and behavioural analysis. For example, if an account is verified or protected, it is a logical indicator that it is a human account, not a bot account. The profile features extracted from the metadata, such as profile image, screen name, and description may also indicate the nature of the account. For example, a default profile image is a new user or a bot account [16].

Table 1 Feature Names

Feature Name	Number of Links
Profile Image	Mention
Tweets Count	# of friends
Retweet	Follower Count
Verified	Age of Count
Favorite Count	User Replies
Lists	Description
Rate of Media	# of words per tweet
Entropy of Tweets	# hastags
URL rate	Screen Name

The temporal pattern, such as the average of tweeting and retweeting ratios, can signify bot activity if it occurs with small inter-arrivals [17]. Therefore, using an entropy component to detect behaviour as part of the classification system is essential. In addition, the rate of posting similar content with URL can be an indicator of a spammer. In other words, the URL feature can be used to detect the link farming behaviour that is typically employed by spammers and bot accounts [18]. Also, using the mention feature in association with the URL and number of link features and tweets' entropy can indicate a bot account with malicious intention. Moreover, if the number of followers is high yet the account is relatively new, the followers are likely fake, and the account is a bot.

Evaluation Parameters

Precision:- Precision value is the ratio of predicted positive user to the total predicted user.

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

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

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

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

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

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

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

CONCLUSIONS

The life of social media depends on real user action, but digital user performs unfair action and reduces overall trust value. Many social sites execute bot detection algorithm. This paper observed that to defend social sites against such bots effectively, one has to fix a set of inherent vulnerabilities found in today's digital network. It collectively represents the enabling factors causing the problem. Paper has reviewed a feature set of social bot detection. It was found that dynamic adopting techniques were more effectively identify the BOT. So in future, a balancing algorithm is required that can balance feature vector and detect BOT behaviour without prior training.

REFERENCES

[1]. Mevada D. L., Daxini V., "An opinion bot analyzer for product Reviews using the supervised machine learning method." pp.03, (2015).

[2]. M. N. Istiaq Ahsan , Tamzid Nahian , Abdullah All Kafi , Md. Ismail Hossain, Faisal Muhammad Shah "Review Bot Detection using Active Learning." 978-1-5090-0996-1, pp.16, (2016).

[3]. Michael C., et al. "Survey of review bot detection using machine learning techniques." Journal of Big Data 2.1, pp.9, (2015).

[4]. Adike R. G., Reddy V, "Detection of Fake Review and Brand Bot Using Data Mining Technique.", pp.02,(2016).

[5]. Rajamohana S. P, Umamaheswari K., Dharani M., Vedackshya R., "Survey of review bot detection using machine learning techniques.",978-1-50905778-8, pp.17 (2017).

[6]. Ameen, A.K.; Kaya, B. Detecting botmers in the Twitter network. Int. J. Appl. Math. Electron. Comput. 2017, 5, 71–75.

[7]. 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).

[8]. B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defences," ACM SIGCOMM Computer Communication Review, vol. 40, pp. 363-374, 2010.

[9]. Y. Boshmaf, K. Beznosov, and M. Ripeanu, "Graph-based Sybil detection in social and information systems," in Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on, 2013, pp. 466-473.

[10]. 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.

[11]. Peining Shi, Zhiyong Zhang And Kim-Kwang Raymond Choo. "Detecting Malicious Social Bots Based on clickstream Sequences". IEEE Access March 18, 2019.

[12]. 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.

[13]. Xueying Zhang, Xianghan Zheng, A Novel Method for Spammer Detection in Social Networks, IEEE,2015.

[14]. M. A. Rajab, J. Zarfoss, F. Monrose and A. Terzis,\ A multifaceted approach to understanding the botnet phenomenon," in Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement (IMC'06), pp. 41-52, 2006.

[15]. 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.

[16]. Alarifi, M. Alsaleh, and A. Al-Salman, "Twitter Turing test: Identifying social machines," Information Sciences, vol. 372, pp. 332-346, 2016.

[17]. Cai, L. Li, and D. Zengi, "Behavior enhanced deep bot detection in social media," in Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on. IEEE, 2017, pp. 128-130.

[18]. M. Chakraborty, S. Pal, R. Pramanik, and C. R. Chowdary, "Recent developments in social spam detection and combating techniques: A survey," Information Processing & Management, vol. 52, no. 6, pp. 1053-1073, 2016.