International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

DETECTION OF MALICIOUS BOTS IN SOCIAL NETWORKS

[1]Mr. K. Venkateswara Rao ,[2]N BHOOMIKA CHOWDARY ,[3]B HARI NARAYANA

[1]Associate Professor, Department of Information Technology, CMR College of Engineering & Technology

[2, 3]B-Tech, Department of Information Technology, CMR College of Engineering & Technology

Abstract:

Malicious social bots generate fake tweets and automate their social relationships either by pretending like a follower or by creating multiple fake accounts with malicious activities. Moreover, malicious social bots post shortened malicious URLs in the tweet in order to redirect the requests of online social networking participants to some malicious servers. Hence, distinguishing malicious social bots from legitimate users is one of the most important tasks in the Twitter network. To detect malicious social bots, extracting URL-based features consumes less amount of time in comparison with social graph-based features. Furthermore, malicious social bots cannot easily manipulate URL redirection chains. Here, a learning automata-based malicious social bot detection (LA-MSBD) algorithm is proposed by integrating a trust computation model with URL-based features for identifying trustworthy participants in the Twitter network.

INTRODUCTION:

Malicious social bot is a software program that pretends to be a real user in online social networks (OSNs). The malicious social bots can manipulate profile features, such as hashtag ratio, follower ratio, URL ratio, and the number of retweets. The malicious social bots can also manipulate tweet-content features, such as sentimental words, emoticons, and most frequent words used in the tweets, by manipulating the content of each tweet. The social relationshipbased features are highly robust because the malicious social bots cannot easily manipulate the social interactions of users in the Twitter network. However, extracting social-relationship based features consumes a huge amount of time due to the massive volume of social network graph. Therefore, identifying the malicious social bots from the legitimate participants is a challenging task in the twitter network.

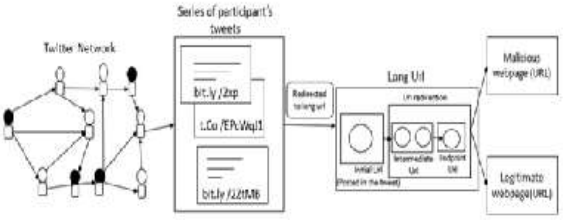

Fig 1 Malicious act on URL shortened service

The proposed framework consists of three components: data collection, feature extraction, and LA model. To collect tweets posted by participants (users), the tweets can be crawled using Twitter Streaming APIs. The data collection component (i.e., phase) consists of three subcomponents (i.e., subphases): reading tweets from Twitter streaming, collecting tweets, and URLs. Moreover, the collected tweets and collected URLs are stored in a repository. The feature extraction consists of two subcomponents: expanding shortened URLs and extracting feature set. Whenever a feature extraction component obtains a shortened URL from the repository, it is converted into a long URL using URL shortened services (such as t.co, bit.ly, and tinyurl.com). For each URL (posted by the participant in the tweet), we extract several features that are based on the lexical properties of URLs (such as spam content and the presence of -, @, and # symbols in the domain name) along with the features of URL redirection (such as URL redirection length and relative position of initial URL). Furthermore, we use these features as input to the proposed LA model for MSBD. The proposed LA model is integrated with a trust evaluation model. Moreover, the trust model determines the probability of a tweet containing any malicious information (such as URL redirection, frequency of URLs, and spam content in URL). Finally, after evaluating the malicious behavior of a series of tweets posted by a participant, we classify tweets as malicious and legitimate tweets. However, malicious tweets are likely to be posted by malicious social bots. This helps in distinguishing malicious social bots from benign participants. The accuracy of the MSBD approach is based on several features that are extracted from the twitter network. 1.1 Problem Statement Malicious social bots perform several malicious attacks, such as spread social spam content, generate fake identities, manipulate online ratings, and perform phishing attacks. In Twitter, when a participant wants to share a tweet containing URL(s) with the neighboring participants the participant adapts URL shortened service in order to reduce the length of URL (because a tweet is restricted up to 140 characters). Approaches that are proposed to detect spam in Twitter Network are:

1. Tweet-Content features
2. Social Relationship features
3. User Profile features

OBJECTIVE :

We propose a methodology to leverage using learning automata for the detection of Malicious Social Bots in Twitter

Network. To protect against the malicious social bot attacks, our proposed LA-based malicious social bot detection (LA-MSBD) algorithm integrates a trust computational model with a set of URL-based features. Finally, we show the effectiveness of algorithm on real software.

IMPLEMENTATION

We are using a dataset from Kaggle. This dataset contains various attributes like URL, description, friends, several followers, a screen name (used to communicate online), location, id, verified (if the user is authenticated), favorite (used for liked tweets), listed count. The data set is trained to identify bots. On this dataset any imbalance of data is removed, features are extracted. For feature independence, the Spearman coefficient is applied. The resulting coefficients; few of them are used in feature extraction and the rest for feature engineering. For feature engineering, a bag of bots' words is fed and applied to the new features. Using these features Decision tree (DT), Logistic regression (LR), K nearest neighbors (KNN), and Naïve Bayes (NB) algorithms are implemented. The algorithm with the highest accuracy is calculated and tested for real-time data.

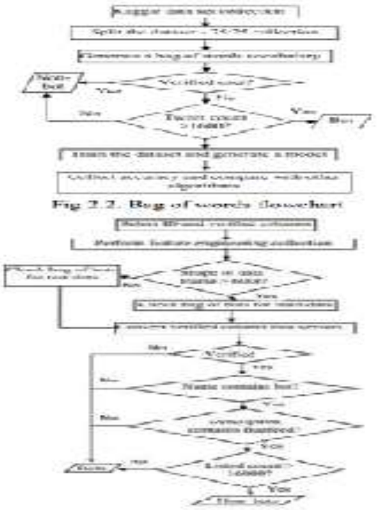

Fig 2 Proposed classifier

PROPOSED MODEL :

Detection of Malicious Bots in Social Networks

Objective The main objective of this proposed model is to identify malicious social bots by analyzing the user behavior in the twitter network. We first propose a framework for analyzing the tweets posted by participants in the Twitter network. In addition, we present a trust model with several features that are extracted from URLs (which are posted by the participants in the tweets) for evaluating the trust value of each participant in Twitter. Finally, an LA-MSBD algorithm is proposed for identifying malicious social bots.Algorithms used for Proposed Model We have used the following algorithms to identify the malicious social bots from the legitimate participants with the help of URL based features:

Feature Ranking Algorithm:

Feature ranking algorithm (with a weight function) helps to identify the most important features based on the weights associated with each feature. Using the weight function, a set of features will be identified as important features, and other set of features will be identified as less influential features based on the available Twitter network data set. For example (i.e., for some data set), spam content, URL redirection length, and relative position of initial URLs may be the most important features, whereas URL without hostname and presence of symbols (like @, -, and #) may be the least influential features for identifying malicious information in tweets. However, the actual set of important features will be determined based on higher weight values on a given data set.

Direct Trust Computation Algorithm:

For MSBD, the direct trust value is evaluated based on identifying the malicious behavior of a participant in terms of posting malicious URLs in the tweets. We consider two classes, namely, malicious and legitimate to train a classifier in order to identify the malicious tweets. We use a Bayesian classifier in order to achieve better precision. We consider feature set with 11 features (for performance evaluation) that are extracted from each tweet. Furthermore, the feature ranking is constructed with the weights associated with each important feature. From the Bayesian learning, we compute the probability that a tweet. We assign weights to each feature before computing the trust value of a tweet because features play a vital role for evaluating the trustworthiness of tweets posted by each participant. Indirect Trust Computation Algorithm: The indirect trust is determined by considering belief values of all one-hop neighbors of a participant. Although the direct trust value is important in evaluating the trustworthiness of the participant, the belief values collected from multiple neighboring participants are also helpful in evaluating the trustworthiness of the participant. Moreover, if legitimate participants randomly add malicious social bots as their friends, then the tweets posted by legitimate participants are likely to be considered as malicious because the legitimate participants are influenced by the malicious social bots. Hence, the belief values collected from the multiple neighboring participants can reduce the bias in the trust value of a participant. The belief value of each one hop neighboring participant is considered as conditionally independent. It is used by DST, where Dempster’s weighted combination rules are applied to determine indirect trust value of a participant in the Twitter network.

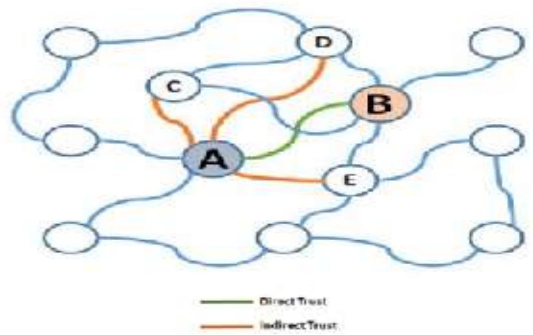

Fig 3 Pointing of Direct & Indirect trust

RESULTS

In the below screen DJANGO webserver started and now open browser and enter URL http://127.0.0.1:8000/ and press enter key to get below output.

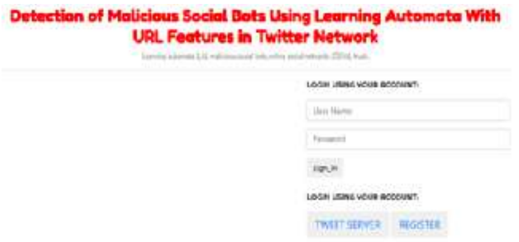
Detection of Malicious Social Bots Using Learning Automata With URL Features in Twitter Network

Fig 4 User Login page

Detection of Malicious Social Bots Using Learning Automata With URL Features in Twitter Network

Fig 6 Users likes result in Pie chart

CONCLUSION :

Our Project aims at developing an LA-MSBD algorithm by integrating a trust computational model with a set of URL-based features for MSBD. In addition, we evaluate the trustworthiness of tweets (posted by each participant) by using the Bayesian learning and DST. Moreover, the proposed LA-MSBD algorithm executes a finite set of learning actions to update action probability value (i.e., probability of a participant posting malicious URLs in the tweets). The proposed LA-MSBD algorithm achieves the advantages of incremental learning. Two Twitter data sets are used to evaluate the performance of our proposed LA-MSBD algorithm.

FUTURE ENHANCEMENT:

Furthermore, as a future research challenge, we would like to investigate the dependence among the features and its impact on MSBD. Future implementations could provide real-time data, which would allow Twitter towards incorporate this function into their app. Additionally, it can be integrated among all other market-available social networking programs. In this project, dataset used for detection is provided through us, & it is entirely manual. However, in future, I may upgrade project so that model can use dataset needed for bot detection on its own.

REFERENCES:

[1].A. Dorri, M. Abadi, and M. Dadfarnia, “SocialBotHunter: Botnet detection in Twitter-like social networking services using semi-supervised collective classification,” in Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Intl Conf Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Aug. 2018, pp. 496–503.

[2].A. Yazidi, O.-C. Granmo, and B. J. Oommen, “Learning-automatonbased online discovery and tracking of spatiotemporal event patterns,” IEEE Trans. Cybern., vol. 43, no. 3, pp. 1118–1130, Jun. 2013.

[3].M. Agarwal and B. Zhou, “Using trust model for detecting malicious activities in Twitter,” in Proc. Int. Conf. Social Comput., Behav.-Cultural Modeling, Predict. Springer, 2014, pp. 207–214.

[4].G. Lingam, R. R. Rout, and D. V. L. N. Somayajulu, “Adaptive deep Q-learning model for detecting social bots and influential users in online social networks,” Appl. Intell., vol. 49, no. 11, pp. 3947–3964, Nov. 2019

[5].P. Shi, Z. Zhang, and K.-K.-R. Choo, “Detecting malicious social bots based on clickstream sequences,” IEEE Access, vol. 7, pp. 28855–28862, 2019.

[6].G. Lingam, R. R. Rout, and D. V. L. N. Somayajulu, “Detection of social botnet using a trust model based on spam content in Twitter network,” in Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS), Dec. 2018, pp. 280–285.

[7]. N. Rndic and P. Laskov, “Practical evasion of a learning-based classifier: A case study,” in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 197–211.

[8].A. Rezvanian, M. Rahmati, and M. R. Meybodi, “Sampling from complex networks using distributed learning automata,” Phys. A, Stat. Mech. Appl., vol. 396, pp. 224–234, Feb. 2014. [9].A. K. Jain and B. B. Gupta, “A machine learning based approach for phishing detection using hyperlinks information,” J. Ambient Intell. Hum. Comput., vol. 10, no. 5, pp. 2015– 2028, May 2019. CMRCET B. Tech (IT) Page No 58 Detection of Malicious Bots in Social Networks

[9]. D. R. Patil and J. B. Patil, “Malicious URLs detection using decision tree classifiers and majority voting technique,” Cybern. Inf. Technol., vol. 18, no. 1, pp. 11–29, Mar. 2018.

[10] Reddy, b. Venkata ramana, nageshbabu dasari, and k. Venkateswararao. "A steganography system with gausian markov random fields and error detection codes." (2021).

[11] Vatambeti, R., Pradhan, N. C., Sandhya, E., Vinta, S. R., Anbarasu, V., & Rao, K. V. Energy Management and Network Traffic Avoidance Using GAODM and E-AODV Protocols in Mobile Ad-Hoc Network.

[12] Revathy, G., Gurumoorthi, E., Sasikala, C., & Latha, T. M. (2023, June). Training superbot with learning automata and multi kernel SVM. In AIP Conference Proceedings (Vol. 2782, No. 1). AIP Publishing.

[13] Gurumoorthi, E., & Ayyasamy, A. (2022). Performance analysis of Geocast based location aided routing using Cache agent in VANET. International Journal of Information Technology, 1-10.

Latha, C. M., & Soujanya, K. L. S. (2018). Enhancing end-to-end device security of internet of things using dynamic cryptographic algorithm. Int. J. Civil Eng. Technol, 9(9), 408-415.

[14] Skandha, S.S., Nicolaides, A., Gupta, S.K., Koppula, V.K., Saba, L., Johri, A.M., Kalra, M.S., Suri, J.S., 2022, A hybrid deep learning paradigm for carotid plaque tissue characterization and its validation in multicenter cohorts using a supercomputer framework, Computers in Biology and Medicine, 10.1016/j.compbiomed.2021.105131

[15] Narsaiah, M.N., Venkat Reddy, D., Bhaskar, T., 2022, Medical Image Fusion by using Different Wavelet Transforms, Lecture Notes in Electrical Engineering, 10.1007/978-981-19-5550-1_33