ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Introduction of a Classification Algorithm Based on features derived from Correlated URLs & TCI for detecting Twitter Mobile Botnets for analyzing Tweet Signature

Sreelakshmi R[#1], Arun P Kuttappan[*2]
[#1] *PG Scholar*
[1] rsreelakshmi23@gmail.com
[*2]*Assistant Professor*
[2]arunkalesh@gmail.com
Department of CSE, Gurudeva Institute Of Science & Technology , Kottyam
APJ Abdul Kalam Technological University
Kerala, India

***Abstract*—Today we all are familiar with many of the online social networking sites such as Facebook , WhatsApp ,Twitter and so on. With the growth of Online Social Networking sites in everyday life, the data shared through social network is in bulk amount and at the same time botnets have invaded the mobile domain. This rise has lead to the crisis of identifying the malicious data. Thus the botmasters uses this platform for their purposes, such as sending spam, gaining control over the network or channel and so on. Twitter is one of the main emerging social network site and many of the tweets in twitter contains malicious sources of information. Here, in this proposed system a detection system is implemented for detecting bot tweets in twitter account by the introduction of a classification algorithm based on features derived from correlated URLs and tweet context information for tweet signature verification.**

Keywords: Social Network Services, Botmasters, TCI, Information Security, Correlation.

I. INTRODUCTION

Today in this modern world, we all know that the mobile phones has become an essential part of our day to day life. It has gradually grown from a simple text and voice device to a fully equipped network which is a platform for running various applications through Internet and also for browsing , and the needs are uncountable. Because of the huge popularity of this OSNs, the invaders has seeded their activities on these platforms, thereby compromising huge devices. The main compromiser, in technical words are called as Bots. These compromised devices are controlled by a Botmaster who is responsible for the attack or invasion.

The social bots is a meticulous type of chatbot that is implemented in a social media networking sites which will generate messages automatically or will act as a follower or will be having a fake account ,pretending to be of genuine thereby causing many phishing type of attacks. There existed many detection system for detecting bottweet. These bots may be automatic or semi automatic that sometimes depends on the human behavior in OSN.A bot in Facebooks was , Facebot that steal information from the device which was infected and use this information which will be encrypted with the bot master's public key so that it won't be accessed other than the bot master. Another bot named Slackbot , which will be activated through a slash command and then it will redeem some confidential data for eg , a customer record from a bank account .

In this paper a detection method to detect Twitter mobile botnets is proposed which will thereby authenticate the tweet signature with a classification algorithm based on the features extracted from correlated URLs and Tweet Context Information. Here two techniques: User Activity Correlation and Artificial Immune System and the introduction of an algorithm used. It can later be developed as an Android app, that can be installed on mobile phones.

The remaining section of the paper is organized as follows: Section II gives a brief idea about the related workson this system, Section III, will describe the Proposed Approach, and the paper can be concluded in Section IV.

II. RELATED WORKS

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

The new threat the social media facing nowadays is Botnet threat.This lead many researchers to work in detecting mobile botnets.To detect these botnets various systems existed. They are described as follows:

Vural and H. Venter, [1] in their research paper named "Combating mobile spam through Botnet detection using artificial immune systems," proposed a for finding bot tweets in Twitter with Artificial Immune System (AIS) detector. The threat which lead to the implementation of this detection system was migration of spamming botnets to mobile devices. Thus inorder to address these problems , a detection system was proposed and it's aim was to introduce novel way of combating threat to mobile devices called as SMS spams. In this method , a software tool was employed with an AIS , in a mobile device. If the detector finds an SMS to be malicious then an alert message is send to the user indicating the message as a suspicious one. If the user agrees that the message is invalid , then an alert message is send to the service provider by the detection system. This detection system was a host based detection system which was harder to manage and they are not suited for detecting network scans and also the can easily be compromised by a DDOS attack.

P. Burghouwt, M. Spruit and H. Sips, [2] , in their paper named, "Towards Detection of Botnet Communication through Social Media by Monitoring User Activity", implemented a method in which botnets in Twitter was detected based on the existence of User Activity. Here a assumption was made as, if a bot visits the social medium, for accessing the information or for uploading any data, the traffic was not controlled by any of the user events. This detection tests , if there was any presence of a user within a particular time frame. If there is no presence of a user, then that tweet is said to be a bot tweet.But the disadvantage of this system was that , eventhough a bot is a legitimate one, it will sometimes be detected as malicious. And it cannot detect a bot which will sometimes be waiting for any user event, called as smart bot, and classifies it as a benign one.

Reham A. and Mostafa H. Dahshan , [3] in their recent work on the paper named "Detecting Social Media Mobile Botnets Using User Activity Correlation and Artificial Immune System", implemented a method by combining both the User Activity Correlation method and Artificial Immune System to detect bot tweets. The presence of User Activity with the Artificial Immune System was a good contribution for the detection of bot tweets. Here the tweet signature is calculated with some of the parameters in the tweet , and then a signature library is maintained ,in which the signatures of the bot tweets are collected and based on this signature, the checking of the tweets happens. But here the problem is that the tweet signature are not collected and authenticated with much accuracy. More parameters should be used to classify the tweet signature which lead to the proposed system.

III. PROPOSED APPROACH

The proposed method combines both UAC & AIS techniques and along with it in AIS detection part, the tweet signature is verified and authenticated with more accuracy by using additional parameters such as:

- Test on URL
- Number of followers
- Number of friends
- URL chain length
- Follower friends ratio
- Account Creation Time
- Activity sequence length

The system takes several steps for the detection process of bot tweets:

1. Capture the tweet sent to the twitter .

2. Calculate the correlation and tweet signature.

3. Compare the correlation value with the threshold value.

4. If the correlation value is high , and ath the same time if there is no match in the signature library , the tweet will be directly send to the user.

5. If there is a match in the signature library, them user will be alerted with a message showing whether to accept the tweet or not.

6. If the user accepts the tweet, then the signature is deleted from the library.

7. If there is no match in the library, and correlation value is very low (negative), the system checks the source list of that application, and if it is in the approved list of applications, the tweet will not be blocked. Otherwise , again a alert message will be given to the user.

A. Capturing Tweets

In the first step, the tweets are captured with the help of a twitter's public stream API and then it is send to our detection system for further process.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

B. UAC Detector

The UAC, User Activity Correlation Detector , will detect the presence of user activities in a certain time frame. When a tweet comes, then the UAC detector checks whether any user activity took place in that given time interval. Here a correlation term is used, which checks the correlation between the time of the tweet send and time of that user activities, A correlation by definition means, it's a single number that will delineate the relation between any two variables. Here , if the correlation value is high, then the tweet will be user generated.

C. AIS Detector

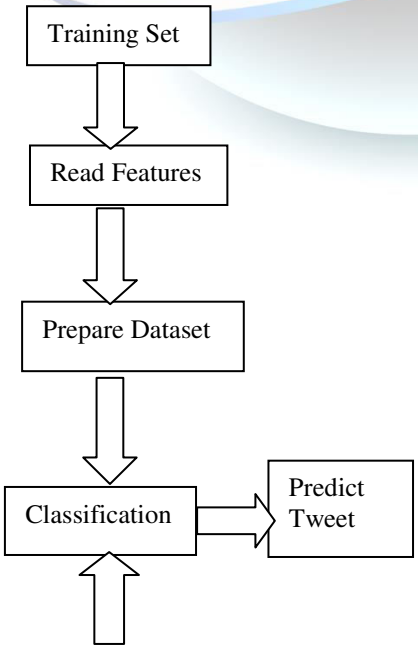
AIS , Artificial Immune System, will classify bot tweets and legitimate tweets , and will give an alert or warning to the user if the mobile is used for sending spam tweets to twitter. In AIS detection part , there comes the tweet signature part and the signature library.

1. Tweet Signature and Signature Library.

The tweet should be converted to a digital format**, so** that we can represent it as a digital representation. For this representation, the tweet is converted, by identifying the newly generated parameters and classify them based on those results.

2. Learning with Positive Data

A distinct characteristics of using AIS is that, for training , positive data are needed. Means, training needs original tweets from twitter account , and based on the match in signature library, AIS detects whether the tweet is genuine or not. The block diagram of the proposed system is shown in Fig. 1



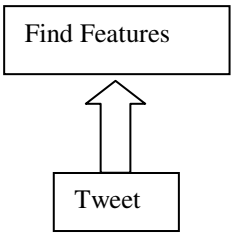


Fig. 1. Block diagram of the proposed method.

The steps in classification of tweets are:

1. URL testing in tweet takes place.
2. No: of friends and followers are noted.
3. Account creation time is taken.
4. Activity sequence length is checked.
5. The ratio between friend and followers ratio is calculated.

Attackers usually use long URL chain s to make investigation little more difficult. Thus whenever an entry point URL is found to be malicious, its chain length of URL will be longer than that of the legitimate URLs. Thus to normalize this function an upper bound value of 20 is chosen. If the length of redirect chain is "l", this feature can be normalized as: min(l,20) / 20.

No: of followers and friends of attackers accounts will mostly be identical, because, attackers mostly use certain type of programs to rise their members in followers and friends list.

Standard deviation of account creation date: Attackers mostly bring a huge number of Twitter accounts within a very short period of time. Therefore, if the account creation dates of the same entry point URL are identical ,it might indicate that the current entry point URL is suspicious.

IV. CONCLUSION

In this paper , we have proposed a detection system for twitter botnets in twitter , where, the tweet signature is verified or authenticated with a classification algorithm which uses the features from correlated URLs and tweet context information. The recent work which used only User Activity Correlation method and Artificial Immune System, was having a drawback, where the tweet signature was derived from simple features .These features are not enough to summarize whether the tweet generated is a bot tweet or benign one. So our proposed system, shows the detection of tweet with more accuracy and can predict whether the tweet is bot or legitimate tweet. Based on this features, we can accept the tweet or if needed we can block those tweets, which will thereby block those tweet's

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

source or sender. This system can be extended to other social media such as Facebook.

REFERENCES

[1] I. Vural and H. Venter, "Combating mobile spam through Botnet detection using artificial immune systems," Journal of Universal Computer Science 18.6, vol. 18, no. 6, pp. 750-774, 2012.

[2] P. Burghouwt, M. Spruit and H. Sips, "Towards Detection of Botnet Communication through Social Media by Monitoring User Activity," in Information Systems Security, vol. 7093, Springer Berlin Heidelberg, 2011, pp. 131-143

.[3] Reham A. and Mostafa H. Dahshan" Detecting Social Media Mobile Botnets Using User Activity Correlation and Artificial Immune System", 2016, IEEE

[4] A. Graaff and A. Engelbrecht, Optimized coverage of non-self with evolved lymphocytes in an artificial immune system, International Journal of Computational Intelligence Research, vol. 2(2), pp. 127– 150, 2006.