Virulent Accounts Detection in Social Network Based Promotions

[1]Priyanka Polagoni, [2]Palaparthy Durga Prasad, [3]Dr. Prasanta Kumar Sahoo

[1,2,3]Dept. of CST, Sreenidhi Institute of Science and Technology, JNTUH University, Telangana, India

Abstract

In Recent years, many of the Social networking sites are dealing with financial capabilities by using the real or virtual currency. They are the advanced platforms where various businesses are being hosted, one such example is online promotion events.The users of social networking sites logs in with their credentials and participate in the online promotion events to get the rewards. Taking this as an advantage attackers control a huge number of accounts to collect the rewards,which results in inefficiency of the system.Thus posing a problem for business people and the social networking sites.In order to overcome this problem a novel system is being proposed which is used to detect and deactivate the malicious accounts that participate in online promotion events before the rewards are being committed by using the features like users general behaviors, their recharging patterns and the usage of their currency.

Keywords

Online Social Networks, Virtual Currency, Malicious Accounts.

I. Introduction

OSNs that integrate with virtual currency presents a new platform for various types of marketing, one such example is online promotion events organized by business entities where users who are recognized by their unique OSN account takes part in the promotions to gain the rewards in the form of virtual currency. Once the rewards are being collected from the promotion events the users can use those rewards for various purposes like transferring the rewards to other users, shopping and even converting it to real money. Such promotion events are useful to the OSN users in many ways and helps in doing the things with ease.

Apart from the advantages it has also got some drawbacks which include malicious accounts participating in the promotion events to collect the virtual currency. The malicious users create multiple set of accounts to participate in the promotions and to collect the money which results in inefficiency of the system, brings loss to the business entities and also ruins the fame of the OSNs. When large amount of virtual currency is being collected by the malicious accounts it poses a great challenge against the virtual currency regulation.These are the important reasons for detecting the malicious users over OSNs. The detection of those malicious users allows the business entities and OSNs to take necessary actions against the attackers like deactivating the accounts before rewards are allotted.

In order to detect the virulent accounts in promotion events a new system is presented which collects the following information from the accounts that participate in the promotion events.The features include a) users social activities b) how OSN users collect virtual currency and c) how the money is spent. After collecting the above features a decision tree classification technique is applied on the above features which classifies the malicious and genuine users.

II. Related Work

Many Techniques have been introduced to find the malicious accounts in the social networking sites.”Detecting clusters of fake accounts in online social networks” Cao xiao [1] introduced a system to find clusters of malicious accounts in online social networking sites. This system uses a pipeline technique to find out clusters of fake accounts. The three important features in pipeline technique are cluster builder, profile feature and Account scorer.with the help of the above three features clusters of fake accounts that send spam messages are detected.”Detecting video spammers in youtube social media” yuhanis yusof [2] devised a system which is used to detect the virulent users who are involved in video spamming over social networks like you tube. A novel combination of features are used based on the edge rank algorithm which is mostly used by the facebook to decide and display popular videos in users news feed. Edge rank algorithm is used to observe the posts and understand the actual content of the posts through its score. Sajid yusof bhat [3] represented a system which uses community related features for exposing spammers over social networks. This system uses a graph classification technique for detecting virulent accounts over social networks. Prof A.R.Gaidhani sagar [4] presented a system to detect malicious accounts and fake reviews in online promotions using knn classification technique.”COMPA detecting compromised accounts on social networks” Manuel Egele [5] came up with a new system to find out the compromised accounts in online social networks and it has been experimented on two famous social networking sites facebook and twitter. This system is composed of two modules. The first one is statistical modelling and the next one is the detection module to find out the accounts which have sudden change in their behavior. A tool named COMPA is used by this system to detect the malicious accounts.

Bhaskar N. Patel, Satish G. Prajapati [6] Efficient classification of data using decision tree. This paper is used to learn about decision tree in brief. ambikesh himansu singh and kiran B.V. [7]introduced a new system to create a social behaviour profile for each social network user account to analyze the behaviour of that particular user. By using the behavioral profiles it is easy to distinguish one user from others.thus helps to find out the compromised accounts over social networks Bandar alghamandi, jason watson, yue xu [8]presented a new system to detect virulent links over social networks using the behaviour of the users.

III. System Design

The proposed system virulent accounts detection in social network based promotions is used to detect the malicious accounts from three prospects which include users general behaviors, their currency collection pattern and their currency expenditure pattern.

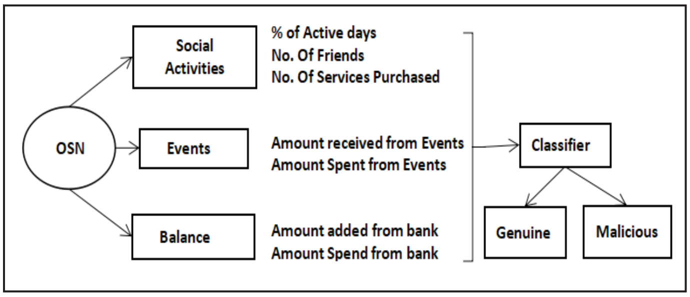


Fig. 1: The Architectural Overview of Our System

A. User Social Activities

User social activities are the very general activities performed by the people over the social networking sites which include chatting with friends sharing the messages photographs with the other users etc.. By observing the users social activities the following features are identified i.e. percentage of active days of the users, number of friends each user is associated with, number of services purchased by the users .

Percentage of active days: If a user logs in to his social networking site account on a particular day then that day is considered as an active day. A genuine user usually logs in every day in the present generation to perform one or the other tasks such as communicating with the friends, sharing the popular news feed etc. Malicious users logs in to his account only during the promotion days to participate in the promotion events and to collect the virtual currency.Therefore the percentage of active days of users helps us to anticipate the malicious users. The percentage of active days graph of malicious users increases only during promotion days and then remains constant where as the same graph of genuine users gradually increases.

Table 1: Percentage of Active Days

User id	User name	Date	Time	count	% of active days
01	Jhon	02-01-2015	01:15 PM	365	100
02	martin	06-01-2015	02:30 PM	300	82
03	Williams	21-02-2015	08:10 AM	250	68
04	Jones	28-02-2015	10:06 AM	50	13
05	Lam	15-03-2015	05:15 PM	40	10
06	Smith	25-03-2015	03:05 PM	350	95
07	Jack	16-04-2015	07:45 PM	365	100
08	Charles	23-04-2015	06:18 AM	30	8
09	Henry	06-05-2015	04:25 PM	320	87
10	Peter	10-04-2015	09:06 PM	340	93

The Number of friends: Every social networking site maintains a friend list for each account to improve the user to user communication. A genuine account has a good number of friends in his friend list to perform the activities like communicating with the friends.Malicious users will not maintain a good number of friends in his friend list because he is interested only in promotion events to collect money, maintaining a good number of friends in his friend list will not help him to collect money. The friend list graph of a genuine user slowly increases from day one where as the friend list graph of malicious users suddenly increases on particular days i.e during promotion days and then remains constant.

Table 2: Number of Friends

User id	User name	Number of friends
01	Jhon	300
02	martin	250
03	Williams	35
04	Jones	150
05	Lam	20
06	Smith	15
07	Jack	80
08	Charles	65
09	Henry	200
10	Peter	10

The number of Services purchased by an account: Social networking sites offers paid services to the users.The users who have purchased those services will get access to the upgraded versions. some of the genuine users like to purchase the services and get upgraded membership. The malicious accounts never wanted to purchase the services because those services will not help the malicious users to collect currency. The services purchased graph of genuine users gradually increases where as the same graph of malicious users remains constant.

B. Currency Collection Features

The users of online social networking sites can collect the money not only by participating in promotion events but also in various ways like transferring the amount from bank account, transfers made between the users, transfers made during buying or selling of goods etc. Generally the genuine users tend to be more active in currency collection when compared to the malicious users, this is because genuine users link their bank account to the online social networking sites and perform transactions whenever necessary where as malicious users aim only for collecting the money from promotion events. The number of transactions from bank account and the number of transactions from the events are observed.If the number of transactions from the bank account are greater than the number of transactions from the events then those accounts tend to be genuine, on the other hand user accounts tend to be malicious if the number of transactions

Table 3: Recharge from Events and Bank

User id	User name	VC from events	Money from bank	total
01	Jhon	100	2000	2100
02	martin	100	5000	5100
03	Williams	200	3000	3200
04	Jones	2500	600	2500
05	Lam	1500	000	1500
06	Smith	180	2600	2780
07	Jack	000	1500	1500
08	Charles	3000	000	3000
09	Henry	300	3500	3800
10	Peter	450	990	1440

from bank are less than the transactions from the promotion activities.

C. Currency expenditure features

This include the total amount spent by an user irrespective of expenditure from bank and expenditure from events.Generally the total currency spent will be more for genuine users because they spend the money from bank account as well as from the events where as the malicious users spend the amount received from the promotion events which is a very small amount.

Table 4: Expenditure from VC and bank

User id	User name	Trans-action id	Expen-diture from bank	Expen-diture from VC	date	time
01	Jhon	Tra01a	2000	100	2-1-2015	02:10PM
02	martin	Tra02b	5000	100	5-2-2015	01:20PM
03	Williams	Tra03c	3000	200	10-3-2015	09:05PM
04	Jones	Tra04d	0000	2500	15-3-2015	05:15AM
05	Lam	Tra05e	0000	1500	22-4-2015	07:40AM
06	Smith	Tra06f	2600	180	30-4-2015	03:35PM
07	Jack	Tra07g	1500	0000	06-5-2015	10:55AM
08	Charles	Tra08h	0000	3000	27-7-2015	06:18PM
09	Henry	Tra09i	3500	300	01-8-2015	08:24PM
10	Peter	Tra10j	990	450	20-8-2015	12:30PM

The Percentage of expenditure from banks: As we already know users can link their bank account to the social networks, most of the genuine users associate their bank accounts with the online social networks and perform shopping, transferring money others etc.. Malicious users will not associate their bank accounts with online social networking sites for two reasons. Firstly, by associating with the bank accounts the identity of the malicious users can be exposed secondly their aim is to collect the money not to spend the money from the bank. Therefore if the percentage of expenditure from bank is greater than the percentage of expenditure from events then those accounts tend to be genuine where as if the percentage of expenditure from bank account is less than the percentage of expenditure from events then those accounts tend to be malicious.

The percentage of Expenditure as gifts: After malicious accounts collect virtual currency from the online promotion activities, they will transfer it to malicious accounts utilized for trading. Sending the web gift vouchers turns into the best choice for malicious accounts to exchange cash for two reasons. firstly, sending on the web gift vouchers inside an OSN as a rule does not bring about any expense. Second, such exchange is autonomous to any bank, along these lines requiring no personal information and thus limiting the exposure of attackers.

IV. Algorithm

The aim of the algorithm is to detect virulent accounts that participate in online promotions before rewards are given. Initially the following features are being extracted from the database. The first step is to find the percentage of active days of the accounts that participate in promotion events.% of Active days=(logged in days/ total days)*100. The next step is to find the number of friends connected with each user an then extract the information about number of services purchased by the users who participate in online promotion events.These three features are related to the users social activities.In the next step the number of recharges made from bank and the number of recharges made from promotion events are extracted. These two features are related to users currency gathering pattern.The next step is to find the percentage of expenditure made by using the amount from bank and also the percentage of expenditure made by using the amount from promotion events.

After extracting all the features, the information gain of all the above features is to be calculated using the formula given below:

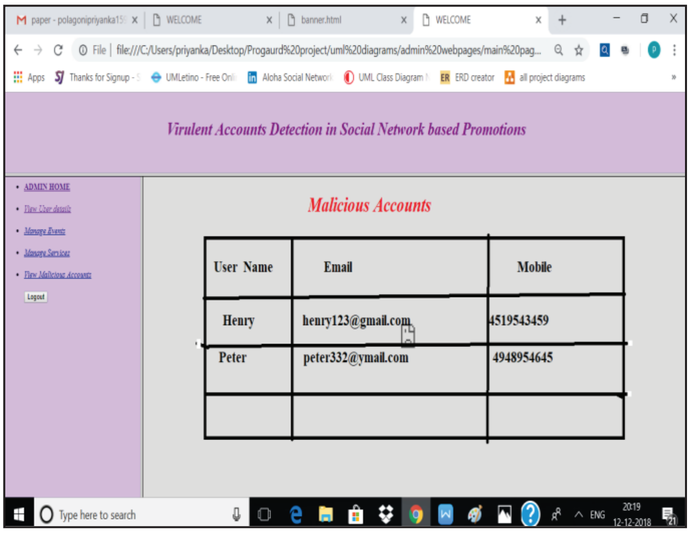
$$\frac{-p}{p+n}log2\left(\frac{p}{p+n}\right)\frac{-n}{p+n}log2\left(\frac{n}{p+n}\right)$$

Once the information gain of all the features is calculated, the next step is to find out the entrophy of records using the formula given below:

$$\sum_{i=1}^{v}\frac{p_i+n_i}{p+n}\left(I\left\langle p_i,n_i\right\rangle\right)$$

After finding the entrophy, the final gain value is calculated using the below equation

Gain = Information gain- Entrophy.



Virulent Accounts Detection in Social Network based Promotions

Malicious Accounts

User Name	Email	Mobile
Henry	henry123@gmail.com	4519543459
Peter	peter332@ymail.com	4948954645

Fig. 2: Result of Virulent Accounts Detection in OSN based Promotions

The entrophy and the gain values helps us in finding the splitting attributes. The attributes which has the highest gain values is considered as the splitting attribute.

Repeat the process until the attributes cannot split further which reveals the malicious and genuine accounts

V. Conclusion

In this paper, decision tree classification technique has been applied on the extracted features to detect the malicious accounts over online social networks. The three main features we have worked with are users general behaviour, users currency collection pattern and users currency expenditure pattern .The results show that this system can detect the virulent accounts before committing the rewards and during the detection we have observed the sudden changes in the behaviour of the malicious users.

References

[1] Cao Xiao, David Mandell Freeman, Theodore Hwa., “Detecting Clusters of Fake Accounts in Online Social Networks”, 2015 University of Washington.

[2] Yuhanis Yusof, Omar Hadeb Sadoon,“Detecting Video Spammers in Youtube Social Media”, University of Malasia 2017.

[3] Sajid Yousuf Bhat, Muhammad Abulaish,“Community-Based Features for Identifying Spammers in Online Social Networks”, 2013 IEEE/ACM.

[4] Prof.A.R.Gaidhani, Sagar Khaire, Rushikesh Shirsat, “Review on Detecting OSN Malicious Account and Fake Reviews in Online Promotions”.

[5] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna,“COMPA Detecting Compromised Accounts on Social Networks”, NDSS Symposium 2013.

[6] Bhaskar N.Patel, Satish.G, Prajapati, Dr. Kamaljit I. Lakhtaria,“Efficient Classification of Data Using Decision Tree”, 2012.

[7] Ambikesh, Himansu Singh, Kiran B.V.,“Detecting Online Social Behaviour of Compromised Account”, 2017.

[8] Bandar Alghamandi, Jason Watson, Yue Xu.,"Towards Detecting Malicious Links in Online Social Networks through User Behaviour”, Queensland University of Technology Australia.