Detecting Malicious Accounts in Online Marketing Based On Social Networks

[1]Mounika Pasumarthi, [2]M. Jaya Ram
[1]M.Tech Student, Department of Computer Science and Engineering,
[2] Associate Professor, Department of CSE,
Universal College of Engineering & Technology, Andhra Pradesh, India.

Abstract - Online social network gradually integrate financial capacity through the use of virtual and virtual currency. They serve as a platform to do new business activities, such as online marketing events, where users can obtain virtual money as a gift to participate in the event. Both OSN and business partners are very concerned when attackers set brands represent to collect coins from the actual event was that the incident was not necessary and causes a financial loss. It will be very important to account for it was the wrong one before marketing the activities online and then reducing the priority of payment. In a copy of this, we should talk about the system, the DMAOMSN, to achieve this goal through the system that takes into account the perspectives of the three characters are in general, payment structures and the use of their currency. We have argued that a set of detailed experimental data is based on the collection of Tencent QQ, OSN is the world that governs financial management and operations are mounted. The results of the experiment suggest that our system can reach a high level of detection is 96.67% and the positive rate is below 0.3%.

I. INTRODUCTION

Social Networking is that integrates a virtual financial platform that becomes attractive to a variety of business activities, which is to promote the interactive online that is active. In particular, the user, represented by his overall OSN-Na account, can receive gifts in the virtual currency system by participating in online marketing activities held by the business unit. Then you can use the payment was in many ways, such as online shopping, for others even the listed money means. These online marketing models with virtual currency enable greater distances provide financial incentives directly to end users and at the same time reduce communication between commercial organizations and financial institutions. As a result, this model of was promised very quickly with high preparation. But it faces a significant threat: attackers can check multiple numbers, or log in to a new account or by going to an account that has been there, participate in a virtual online currency exchange campaign event. If malicious activity essentially destroys advertising, immediately eliminates the effectiveness of marketing investment by a commercial entity, in the meantime it will destroy ON's reputation. In addition, a large number of virtual currencies, which are dominated by attackers, and have potential challenges to the control of e-money?

Therefore, the account precipitation controls that were attacked by the attack on online marketing activities become important. In this discussion, we see the account as an account that is wrong. Negative positive detection allows NSOs and business organizations to take measures to prevent such account from being banned or reducing the possibility of financing these funds. However, design detection methods are good for listening to some of the most important challenges. First, attackers do not have to serve malicious content (such as phishing URLs and bad implementation) to launch an attack successfully. On the contrary, attackers can carry out attacks simply by clicking on a link provided by business unit or sharing content with business partners. Document itself is not completely different from the account are not supported. Second, the attack succeeds does not have to depend on social structures (for example, the "friends" in the popular "post" or social network). For more specific, it is not good for strikers to maintain the social structure that is active, which basically differ from attack as popular spammers in online social networks. Two challenges this invention makes OSN realize that there must be a very different culture and the discovery of an accident such as spam and fraud. As a result, very difficult to use methods that are to detect spam and account fraud.

To be effective in detecting malicious activity for marketing online and overcoming challenges, we have created a new system called DMAOMSN. DMAOMSN uses a collection of features for that account's behavior to participate in online advertising. These assets are accounted for in a three-tiered account, including i) regular profile usage, ii) virtual fundraising accounts, and iii) virtual money used. DMAOMSN further integrates these features into a classification of data that can be used together to differentiate between attacker controlled accounts and side by side. As we know, this work represents a first-hand effort to detect malicious accounts used for online advertising. We evaluate our system using data collected from Tencent QQ, a leading

online social network in China that uses accepted virtual currency (ie Q currencies), to support the financial agency's activities for large online accounts with 899 million accounts. We showed that DMAOMSN can achieve high detection rates of 96.67% and a positive amount of 0.3%.

II. LITERATURE SURVEY

Human-currency interaction: learning from virtual currency use in china

What happened when the HCl and the money intersected? This article is an analysis of the ethnographic return on the use of natural currency in China to discuss the structure of the game media and the more detailed structure of HCl. We find that the virtual currency acquired, accessed and used can change the behavior and experience of the players. Real and virtual currency can interact in a complex way that increase, expand and value / or and the game character of the world. Integrating money into the HCI problems produce truth, honesty and justice, in order to listen to the challenges and opportunities for the new experience of the innovative consumer.

Online social spammer detection

In this document, we present a general optimization system for collectively using web content information and extensive community spammers and providing an online process solution is effective. The results of the collection of experimental information on Twitter ensure the effectiveness of the proposed system.

Collective Spammer detection in evolving multi-relational social networks

We use examples of random Markov field statistics and reduce the loss factor (HL-MRF), the layers of graphic game models are very scalable. We use Jeka Lab Build and Probability Soft Logic (PSL) for prototypes and experimental data processing solutions the size of Internet Tag.com. Our experiments have shown the effectiveness of our system, which suggests that a model contains a relationship-relationship model that does not connect to the social network to complete performance, is more important to those who do not.

Spam filtering in twitter using sender-receiver relationship

This means that spammers will only be detected when sending spam messages. In this article, we propose a new spam filtering system that contributes spam on Twitter. Instead of using an account, we use a relationship, such as the distance and communication between the sender of the message and the recipient of the message, to determine whether the message is spam now or not. Unlike accounts, connections are difficult for spammers to run and can be collected automatically. We collect a large number of Twitter messages are unwanted and unwanted and then make several comparisons. From our analysis, getting the most spam comes from the cause of a poor relationship with the recipient. In addition, we indicated that our program is more suitable for tracking waste on Twitter from the previous program.

Fraud detection using self-organizing map visualizing the user profiles

We recommend methods to detect fraud based on the display of user accounts and track the type of fee. Display technology used in our strategy is self-mapping (SOM). Because the MOS technology system was originally only to see the vector, and the user account presented in our work as a branch of the store is a collection of records that show the user's operation flow, a form is recommended visual to produce a matrix grid in the SOM, which is an important contribution to the document. In addition, a method is proposed to establish the value based on the detection SOM U-matrix. The results of the pilot are made in real data in three different areas of research to ensure profits and effective methods have been proposed.

III. OVERVIEW OF THE SYSTEM

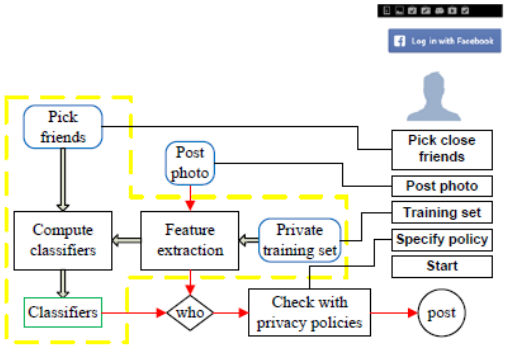

Fig. 4: System structure of our application

Fig 3.1 System Architecture

3.1 EXISTING SYSTEM:

- While social networks on the Internet play a more important role in the cyber world and business, users of evil in NSO become very important. Therefore, many detection methods have been proposed. Due to the popularity of spammers in NSO, the focus was solely on checking accounts that send malicious content. Spam attacks can be viewed as a flow of information initiated by the attackers through a series of malicious accounts

and ultimately into the victim's account.

- Although the cable box this method, they typically use one or three sources of discovery, including i) content in spam messages, ii) Internet infrastructure that makes bad news (for example, phishing or exploitation content), and iii) the social structure between bad accounts and victim accounts.

3.2 DISADVANTAGES OF EXISTING SYSTEM:

But the face of the threat is serious: attackers can control several numbers, or register for a new account or leave the account, to participate in online campaign funds online.

3.3 PROPOSED SYSTEM:

To get better because of poor online marketing activities by overcoming the challenges we are creating a new system, the DMAOMSN. DMAOMSN uses a set of services to make your profile attractive for online campaign activities. This feature aims to distinguish the account from three things, including i) all user profiles, ii) how the account accumulates virtual currency, and iii) how the currency actually was. DMAOMSN further integration of these services with the help of a statistical classification that can be used to distinguish between accounts that are controlled and attack males.

3.4 ADVANTAGES OF PROPOSED SYSTEM:

- This task represents the first systematic effort to detect malicious account used for online promotional activities.
- The results of our experiment suggest that DMAOMSN can reach the high level detection level of 99.67 percent and 0.3 percent positive.

3.5 IMPLEMENTATION

Modules:

Bank Admin

In this theme, the controller must log in with a name and password, the keyword is illegal. Once to the right, you can perform a number of activities, such as All users' opinions and permissions, view all merchants and permissions, set availability and view, see all bad users based on product purchase (users try to buy unevenly) stop if you do it out of bounds for access, see all evil users due to number of transfers (users trying to change user are not horizontal) and block if they do so outside of bounds of access, list all bad vendors and detailed software and specifying an archery account was like a spam account and block this user, check the removal and opening requirements for users and suppliers, see the number of users and users in the risk zone. Usually on the chart to see the product classification in the chart

- **User**

There are some users in this model. Users must register for the choice of activities before taking any. After registering successfully, you must wait to receive approval and admin after fixed administration. He can sign with my name and password. Logan did that he was going to take a few steps - register on the site and go and if blocked. Look at the type of profile and your account (bad or normal, so the bank account, account to see, check this subscription, find friends and find friends, authorization, see your friends, search for a word and see more information, for Buy the product, move it away to your friends.

- **Seller**

In this theme there are a number of users. Vendors must register with the Election Group before conducting multiple transactions. Once you have registered in the registry, you must wait for administrators to give permission and after the administrator has allowed. You can log in with your username and password. In special log you will run several activities such as View profile and account type, add product using color, pname, manufacturer, DESC use file search, file name, Sprice, bus, image, view object and title and attributes for all users who buy Bill and generally registered poorly (users try to buy for free).

IV. SYSTEM DESIGN

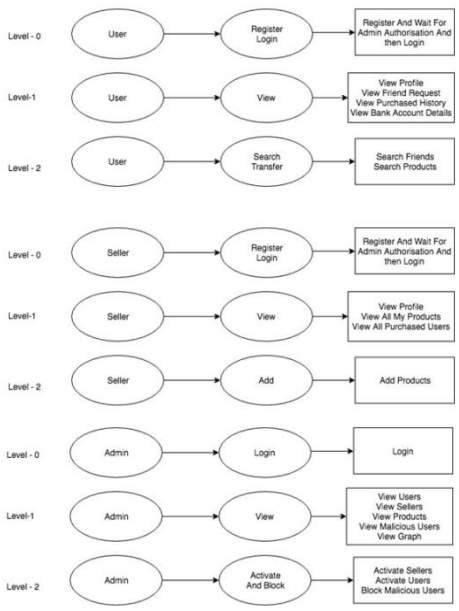

Fig 4.1: Data Flow Diagram

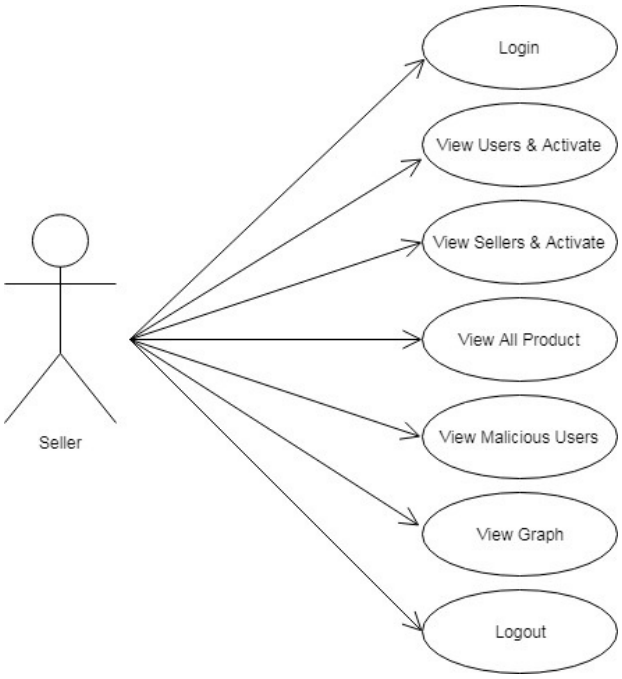

Fig 4.2: Usecase Diagram of seller

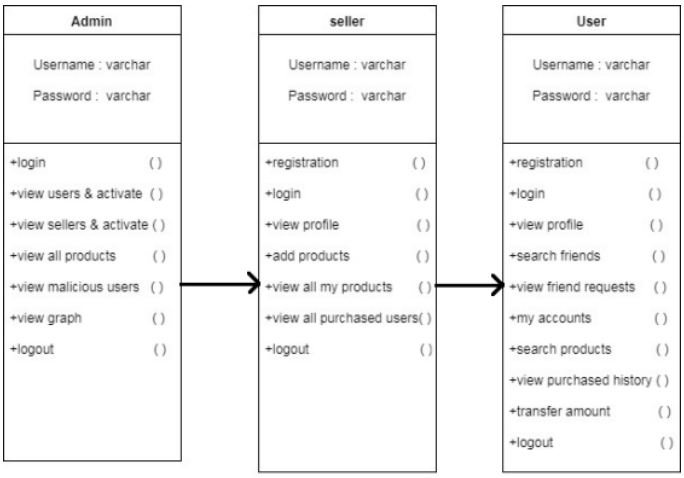

Fig 4.3: Class Diagram

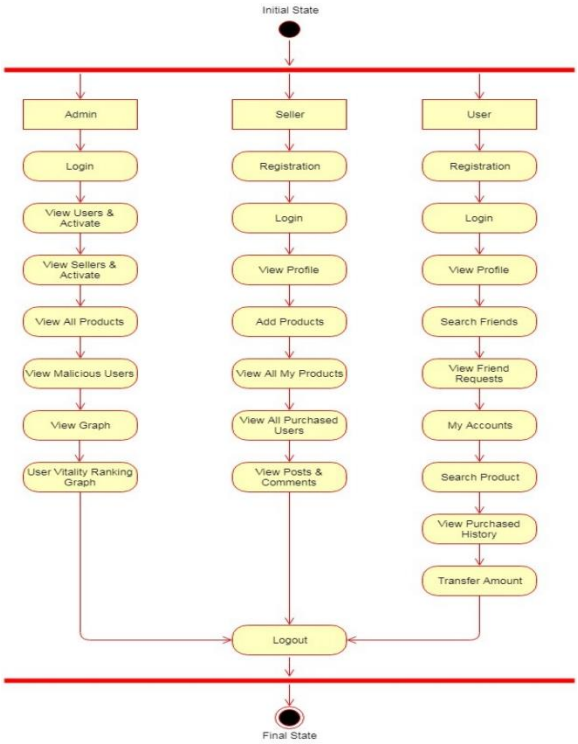

Fig 4.4: Activity Diagram

V. OUTPUT SCREEN SHOTS

Fig 5.1: Home Page

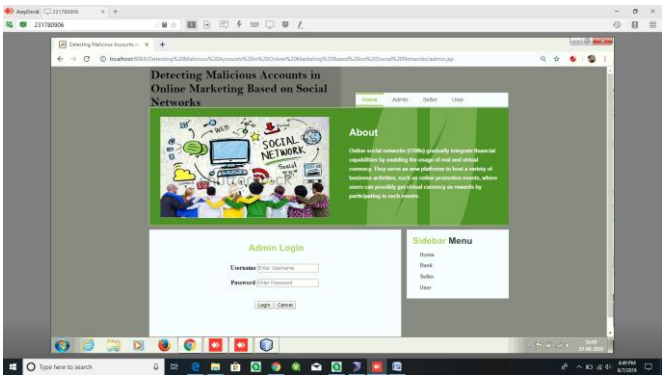

Fig 5.2: Admin login Page

Fig 5.3: Admin home Page

Fig 5.4: View users and activate Page

Fig 5.5: View seller and active Page

Fig 5.6: View products Page

Fig 5.7: View Malicious Users Page

VI. CONCLUSION AND FUTURE SCOPE

This document introduced a new system, DMAOMSN, to automatically detect your NSO that wants to participate in the activities of the online campaign. DMAOMSN uses three types of services, as well as the character in general, a virtual currency collection and use the virtual currency. The results of

the experiment based on reference data collected from Tencent QQ, a leading company in the OSN world, demonstrated the DMAOMSN accuracy, which reaches a high detection rate of 96.67% remember one of the lowest-positive is the most down 0.3%.

VII. REFERENCES

[1] Y. Wang and S. D. Mainwaring, "Human-currency interaction: learning from virtual currency use in china," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.

[2] J. S. Gans and H. Halaburda, "Some economics of private digital currency," Rotman School of Management Working Paper, no. 2297296, 2013.

[3] X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65.

[4] "Leveraging knowledge across media for spammer detection in microblogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 2014, pp. 547–556.

[5] 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.

[6] Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog or block: Detecting blog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

[7] S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, "Collective spammer detection in evolving multi-relational social networks," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769–1778.

[8] Y.-R. Chen and H.-H. Chen, "Opinion spammer detection in web forum," in Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2015, pp. 759–762.

[9] F. Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in microblogging with social context regularization," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610.

[10] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering,"