IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 8, August 2020, ||Series -I|| PP 25-33

Identtifying Unauthorised Account in Social Networking Online Campaigning

BAAKI DURGA SRAVANI[1], Dr.P.BALA KRISHNA PRASAD[2], Dr. GOPISETTI GURU KESAVA DASU[3]

[1] M.Tech Scholar, Department of Computer Science Engineering,
[2]Professor & principal Eluru College of engineering and technology, ap, india.
[3]Professor and Hod Department of Cse, Eluru College of Engineering and Technology, Ap, India.

Received 12 August 2020; Accepted 28 August 2020

ABSTRACT: Online social networks (OSNs) gradually integrate nancial capabilities by enabling the usage of material and virtual currency. They attend as new programs to host a variety of business activities, such as online promotion events, where users can possibly get virtual currency as rewards by taking part in such consequences. Both OSNs and business partners are signicantly concerned when attackers instrument a set of scores to collect virtual currency from these cases, which cause these events ineffective and result in sign can't nancial loss. It becomes of great importance to proactively detect these malicious accounts before the online promotion activities and subsequently decreases their priority to be paid back. In this report, we suggest a novel arrangement, namely ProGuard, to achieve this objective by systematically integrating features that characterize accounts from three perspectives, including their general behaviors, their recharging patterns, and the exercise of their currency. We have done extensive experiments based on data gathered from the Tencent QQ, a global leading OSN with built-in nancial management activities. Experimental results have shown that our system can achieve a high detection rate of 96.67% at a very low false positive rate of 0.3%.

INDEX TERMS: Online social networks, virtual currency, malicious accounts.

I. INTRODUCTION

Online social networks (OSNs) that integrate virtual currency serve as an appealing platform for various business actions, where online, interactive promotion is among the most dynamic singles. Space Cally, a user, who is normally presented by her OSN account, can possibly get rewards in the sort of virtual currency by participating online promotion activities organized by business entities. She can then use such reward in various ways, such as online shopping, transporting it to others, and even switching it for real currency [1]. Such virtual-currency-enabled online promotion model enables enormous outreach, offers direct nancial stimuli to end users, and meanwhile minimizes the interactions between business entities and nancial institutions. As a consequence, this model has indicated outstanding promise and gained huge prevalence rapidly. Nonetheless, it faces a semi can't threat: attackers can manipulate a heavy number of stories, either by registering new accounts or compromising existing account, to participate in the online promotion results for virtual currency. Such malicious activities will fundamentally weaken the strength of the promotion activities, immediately voiding the effectiveness of the promotion investment from business entities and meanwhile damaging ONSs' reputation. Moreover, a large volume of virtual currency, when controlled by attackers, could also become a potential challenge against virtual cur-rency regulation [2].

It therefore becomes of essential importance to detect accounts controlled by attackers in online promotion activities. In the following discussions, we cite to such accounts as malicious accounts. The effective detection of malicious accounts enables both OSNs and business entities to take mitigation actions such as casting out these accounts or decreasing the possibility to reward these accounts. Still, planning an effective detection method is faced with a few semi can't challenges. First, attackers do not require to generate malicious content (e.g., phishing URLs and malicious executables) to launch successful attacks. Comparatively, attackers can effectively perform attacks by simply clicking links offered by business entities or sharing the benign content that is originally passed out by the business partners. These natural processes themselves do not perceivably differentiate from benign accounts. Second, successful attacks do not need to depend on societal constructions (e.g., ‘‘following’’ or ‘‘friend’’ relationship with popular social networks). To be more space c, maintaining active social structures does not ban t to attackers, which is essentially different from popular attacks such as spammers in online social nets. These two challenges make the detection of such malicious OSN accounts, fundamentally different from the detection of traditional approaches such as spamming and phishing. As a result, it is exceedingly difficult to adopt existing methods to detect junk e-mail and phishing accounts.

In parliamentary law to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel strategy, namely ProGuard. *ProGuard* *employs a collection of behavioral features to pro lean account that takes part in an online promotion event.* These characteristics aim to restrict an account from three aspects including i) its general usage pro Leo, ii) how an account collects virtual currency, and iii) how the virtual currency is spent. *ProGuard further integrates these features using a statistical classier so that they can be collectively used to distinguish between those accounts controlled by attackers and benign ones.* To the best of our knowledge, this work represents the rest try to systematically detect malicious accounts used for online promotion activity participation. We have evaluated our system using information collected from Tencent QQ, a leading Chinese online social network that employs a widely-accepted virtual currency (i.e., Q coin), to support online nancial activities for a giant body of 899 million active accounts. Our experimental results have demonstrated that *ProGuard* can achieve a high detection rate of 96.67% with a very low false positive rate of 0.3%.

II. RELATED WORK

Since online social networks play an increasing important role in both cyber and business world, detecting malicious users in OSNs becomes of great importance. Many detection methods have been consequently proposed [3] [10]. Seeing the popularity of spammers in OSNs, these methods almost exclusively concentrate on detecting accounts that send malicious content. A spamming attack can be viewed as an information now initiated from an attacker, through a serial publication of malicious accounts, and Nally to a victim's report. Despite the diversity of these methods, they generally leverage part or wholly of three sources for detection, including i) the content of the spam message, ii) the network infrastructure that hosts the malicious data (e.g., phishing content or exploits), and iii) the social structure among malicious accounts and victim accounts. For example, Gao et al. [11] designed a method to reveal campaigns of the malicious accounts by clustering accounts that send messages with similar capacity. Lee and Kim [12] devised a method to rest track HTTP redirection chains initiated from URLs embedded in an OSN message, then grouped messages that led to webpages hosted in the same host, and Nally used the server reputation to identify malicious accounts. Yang et al. [13] extracted a graph of the ‘‘following’’ relationship of twitter accounts and then propagated maliciousness score using the derived graph; Wu et al. [9] Proposed a social spammer and spam message co-detection method based on the posting relations between users and messages, and utilized the relationship between the user and the message to improve the functioning of both social spammer detection. Compared to existing methods of detecting spamming accounts in OSNs, it is faced with new challenges to detect malicious accounts that participate in online promotion activities. First, different from spamming accounts, these explanations, neither rely on spamming messages nor need malicious network infrastructures to launch attacks. Second, social structures are not necessary. Consequently, none of the existing methods are applicable to detecting malicious accounts in online pro-movement activities. To solve the new challenges, our method detects malicious accounts by looking into both regular activities of an invoice and its mainsail activities.

However, we consider our method and existing approaches can complement each other to improve the security of online social networks.

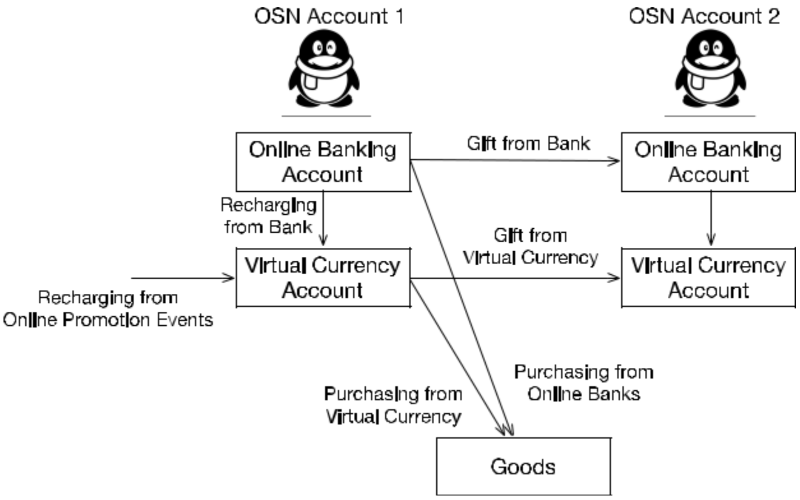


FIGURE 1. The integration of OSN accounts and financial accounts

III. BACKGROUND

In an OSN that integrates nancial activities, an OSN account is ordinarily connected with invoices for both online banking and virtual currency. Number 1 presents such an example, where a QQ account, the most popular OSN account of Tencent, is linked with an online banking history for real currency and an account for virtual currency (i.e., Q coin). A user usually direct deposits real currency into her online banking history; she can recharge her virtual currency account from her banking account. By participating online promotional events, a user can also recharge her virtual currency account by collecting rewards from the promotional events. A user can expend from his accounts in two distinctive ways. Foremost, she can use real or virtual currency to purchase both real and virtual goods (i.e., online shopping). Second, she can transfer both real and virtual currencies to another user by sending out gifts.

Figure 2 presents the typical virtual currency ow when malicious accounts participate in online promotion events. The owl is composed of three phases, including i) collecting,

ii) multilayer transferring, and iii) laundering the virtual currency. In rst phase, an attacker controls a set of accounts to participate in online business promotion activities and each account possibly gets a certain amount of virtual currency as return. In the second phase, the attacker will instrument these currency collection accounts to transfer the virtual currency to other accounts. Multiple layers of transferring activities might be involved to obfuscate the identities of the malicious accounts used for participating online promotion activities. At the conclusion of the second stage, a big measure of virtual currency will be aggregated into a few laundering accounts. In the third stage, the attacker will control the laundering accounts to sell the virtual currency into real hard currency by trading it to individual purchasers.

iii) In parliamentary law to compete with regulated sources for virtual currency (i.e., purchasing virtual currency using real currency), the attackers usually offer a considerable price reduction.

iv)

v) Our aim is to design a detection system capable of identifying malicious accounts that participate in online pro-motion effects for virtual currency collection (at the collection phase) before rewards are given. Detecting malicious accounts at this special c time point (i.e., before the commitment of rewards and at the collection phase) results in unique advantages. Foremost, as a simple heuristic to prevent freshly registered accounts that are likely to be bots, business entities usually require the participating accounts to be read for a certain quantity of time (e.g., a few weeks). Thence, the detected and mitigated malicious accounts cannot be directly substituted by the newly registered accounts, thereby drastically limiting attackers' capabilities. In contrast, no restraint is used for accounts used for virtual currency transferring and laundering. This means such accounts can be easily replaced by attackers if detected, resulting negligible impact to attackers' capabilities. Second, our detection system will mark whether an account is malicious when it participates in an online promotion event; this enables business entities to make actionable decisions such as de-prioritize this account from being rewarded with this outcome. Thus, it can proactively mitigate the nancial loss faced by business entities.

IV. DATA

We have collected labelled data from Tencent QQ, a leading Chinese online social net that provides a kind of inspection and repairs such as instant message, voice chat, online games, online shopping, and e-commerce. All these services support the use of the Q coin, the virtual currency distributed and managed by Tencent QQ. Tencent QQ has a giant body of 899 million active QQ accounts with a reportedly peak of 176.4 million simultaneous online QQ users. Tencent QQ is one of the global leading OSNs that are actively involved in virtual-currency based online promotion activities.

Our data set is composed of 28,000 malicious accounts and 28,000 benign accounts, where all of these scores are randomly sampled from the accounts that participated in Tencent QQ online promotion activities in August 2015. The labeling process starts from identifying laundering accounts (i.e., invoices that are associated with virtual currency spams and accounts that sell virtual currency on major e-commerce sites). Spacecally, if an account removes the virtual currency to any account that engages in virtual-money laundering activities, this score will be labeled as malicious. The understanding is that the target of our detection system is to identify malicious accounts before the rewards are committed.

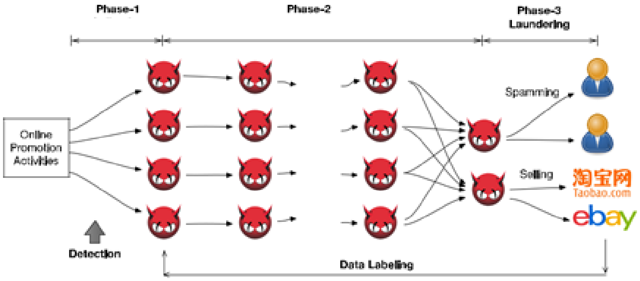


FIGURE 2. Virtual currency flow for malicious OSN accounts.

The upper side of Figure 3 shows the temporal relationship among the data collection procedure, online promotion events, and the account labeling process. Thus, it is worth mentioning that an explanation may not possess any historical nancial activities (even for virtual currency collection activities) since it participates in the online promotion for the relaxation time.

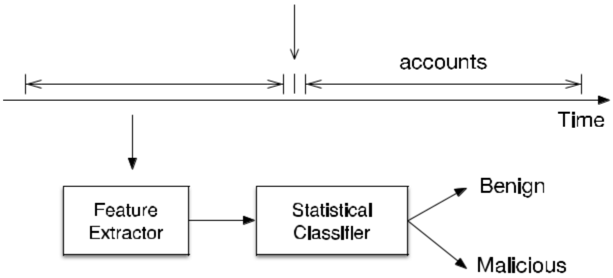


FIGURE 3. The architectural overview of the system.

Although the aforementioned ‘‘trace-back’’ method is effective in manually labeling malicious accounts, utilizing it as a detection method is impractical. Foremost, it takes a terrible quantity of manual efforts for forensic analysis, such as identifying suspicious virtual-currency dealers in external e-commerce websites, correlating spamming content with user accounts, and correlating sellers' pro lens with user stories. In addition, evidence for such forensic analysis will be only available after malicious accounts participate in online promotion results. Thus, this data labeling process, if employed as detection method, cannot guide, business entities mitigate their nancial loss proactively. For each account, we pile up a mixture of data, including 1) login activities, 2) a list of anonymized accounts that this bill has sent instant messages to, 3) service purchase activities, 4) the recharging activities, and 5) the expenditure activities.

V. SYSTEM DESIGN

ProGuardis composed of two phases, namely the trainingphase and the detection phase. In the training phase, a statistical classier learns from a band of pre-labelled malicious and benign explanations. In the detection phase, an unknown account will result is changed to a feature vector and then examined by the statistical classier to assess its maliciousness. The rear end of Figure 3 shows the architectural overview of ProGuard. As a form of statistical classes have been evolved and widely used, designing features capable of dis-criminating between malicious accounts and benign accounts becomes of central focus. In this part, we will present several characteristics and demonstrate their effectiveness on differentiating malicious accounts from benign ones. We offer three general guidelines to direct the feature design.

General Behaviors: Benign accounts are commonly applied by regular users for a mixture of actions such as chatting, picture sharing, and nancial activities. In contrast, malicious news reports are more probable to be driven by online promotion results. Consequently, the benign accounts tend to be more socially active compared to malicious accounts.

Currency Collection: The malicious accounts under investigation focus on using online promotion activities to collect virtual currency. In contrast, benign users are likely to obtain virtual currency from multiple resources.

Currency Usage: Attackers' ultimate objective is to monetize the virtual currency. In contrast, benign users use their virtual currency in much more diversied ways.

A. GENERAL-BEHAVIOR FEATURES

Malicious accounts tend to be less active compared to benign accounts with regard to the non- nancial usage. The attackers usually control their accounts to only participate in online promotion activities. In contrast, benign accounts are more likely to engage in dynamic interaction with other users.

Feature 1: The Ratio of Active Days. This feature presents the proportion of the number of active days of an account for the passed one year. Specically, if an account is logged in at least once for a day, this day will be labeled as ‘‘active’’ for this account.

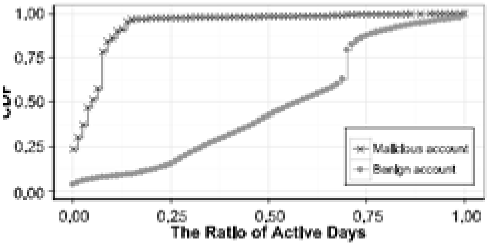


FIGURE 4. Feature 1 - the ratio of active days.

The attackers usually login malicious accounts for participating in online promotion activities that involve virtual currency. Thus, malicious news reports tend to be understood in the absence of online promotion activities. The availability of promotional activities is significantly in uenced by timing and spatial components. As a result, malicious news reports tend to be inactive generally. Comparatively, benign accounts are applied by regular users and their logins are driven by the daily usage such as visiting and picture sharing. Many users configure their applications to automatically login upon the bootstrap of the underlying system (e.g., a smartphone), which further facilitates volatility of benign accounts. Figure 4 gives the distribution of feature values for both malicious accounts and benign explanations. As exemplified in the four, the vast majority of the malicious accounts (i.e., roughly 98% of malicious accounts) are active for less than 20% of total days, whereas only a smaller part of benign accounts (i.e., less than 20%) experience the same activity level (i.e., being alive for less than 20% of one year).

B. CURRENCY COLLECTION FEATURES

In addition to collecting virtual currency by taking part in online promotion activities, an OSN user can recharge her account with virtual currency through various ways such as wire transfer, selling virtual goods, and transmitting from other stories. More often than not, benign users should be more dynamic with respect to recharging their accounts. We suggest two features to characterize this movement from two aspects including the amount of recharging and the important sources for recharging.

Feature 2 - The Average Recharge Amount of Virtual Currency. This feature maps the mean sum of virtual currency for each recharge regardless of the sources for recharging.
Benign users who take part in online promotion activities are usually also interested in other online nancial activities. Thus, these benign users tend to actively recharge their accounts. The recharge amount for each time by a benign user is commonly considerably large since users tend to lessen the hassle of recharging. In contrast, if a malicious account has been recharged, the quantity of virtual currency for each recharge is normally limited by a comparatively small volume offered by the online promotion activity. Figure 7 shows the distribution of this feature for benign and malicious accounts, respectively. Space Cally, the average recharge amount is higher than 1100 Chinese cents1 for more than 50% of benign users, where only a minuscule part (i.e., about 15%) of malicious users have an average amount that is higher than 140 Chinese cents.

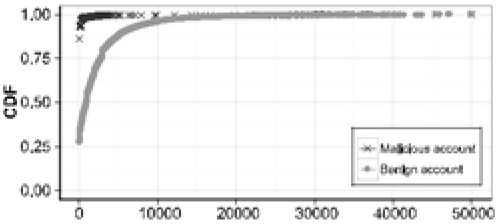


FIGURE 5. Feature 4 - the average recharge amount.

VI. EVALUATION

We performed extensive evaluation of *ProGuard*, which focuses on the overall detection accuracy, the importance Of each feature, and the correlation between these features. For this evaluation, we used totally 56,000 accounts whose entire dataset are divided into 28,000 malicious accounts and 28,000 benign accounts. Such data serve as a well-balanced dataset for training a statistical classier [19].

A. DETECTION ACCURACY

We have used the normalized Random Forest (RF) as the statistical classier for *ProGuard* and evaluated its detection accuracy. RF classier [20] is an ensemble of unpruned classification trees, which is trained over bootstrapped samples of the original data and the prediction is built by aggregating majority vote of the ensemble. In parliamentary law to ward off the prejudice caused by the choice of specific training set, we also performed 10-fold cross validation. Specically, the entire dataset is partitioned into 10 equal-size sets (i.e., 10-folds); then iteratively 9-folds are used for training and the remaining 1-fold is adopted for testing. The RF classier was trained with 3000 trees and randomly sampled 4 features for each of tree splitting [21]. The receiver operating characteristic (ROC) that characterizes the overall detection performance of *ProGuard* is presented in Fig. 12. The experimental results have shown that *ProGuard* can achieve high detection accuracy. For example, given the false positive rate of 0.3%, *ProGuard*can accomplish a high detection rate of 96.67%.

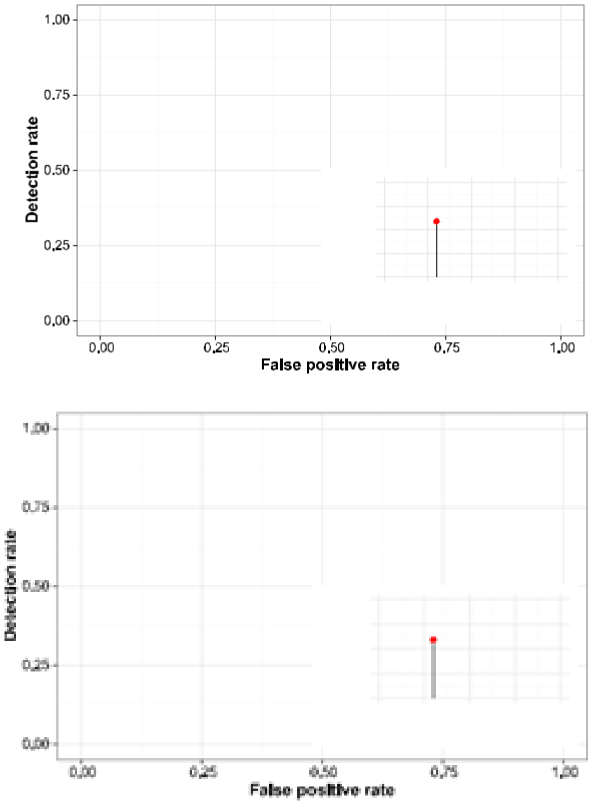


FIGURE 6. ROC curve on 8 features.

In practice, alternatively statistical classes might be adopted to render new performance being teas such as scalability. Therefore, we also evaluate how *ProGuard* performs when alternative, classic ears are used. As a means towards this end, we used Support Vector Machine (SVM) [22] and Gradient-Boosted Tree [23] to repeat our experiments. Specically, we used 10-fold cross validation for each of classiers and calculated the area under the ROC curve (AUC) [24], a widely used measure of quality of super-vised classication models, which is equal to the probability that a randomly chosen sample of malicious accounts will have a higher estimated probability of belonging to malicious accounts than a randomly chosen sample of benign accounts. Since AUC is cutoff independent and values of AUC range from 0.5 (no predictive ability) to 1.0 (perfect predictive ability), a higher AUC of a classier indicates the better prediction performance, irrespective of the cutoff selection.

Table 1 lists the AUC values for all three classiers used in the experiments. Both SVM and Gradient-Boosted Tree accomplished high detection results, comparable with the Random Forest which has the best performance on AUC. The experimental results imply that our proposed features are not sensitive to the selection of statistical classiers.

TABLE 1. AUCs for three classifiers.

Classifier	AUC
Random Forest	0.9959
SVM	0.9753
Gradient-Boosted Tree	0.9781

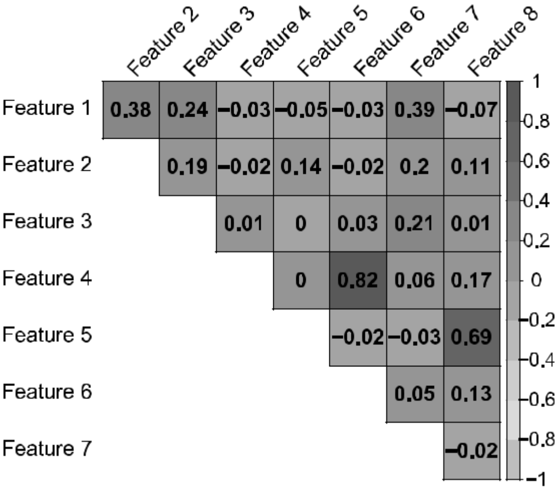
B. FEATURE IMPORTANCE AND CORRELATION

We investigated the relative importance of the proposed fea-tures in the context of Random Forest classifier, which has accomplished the best detection accuracy according to our experiments. We employed the variable importance of each feature to the Random Forest classification model using per-mutation test [21]. The variable importance for each feature is computed by mean decrease in accuracy, which is defined as a prediction error rate after permuting an each feature [21]. The rank of features based on the variable importance is shown in Table 2. Specifically, the ratio of active days (Feature 1), the average recharge amount of virtual currency (Feature 4), and the percentage of expenditure from banks (Feature 7) represent the most significantly for detection. It is worth not-ing that these top three features cover three complementary aspects including the general behaviors, currency collection, and currency usage that guide the feature design.

TABLE 2. Feature importance rank of **Pro Guard** by random forest.

Rank	Variable importance
Feature 1	465.4
Feature 4	349.9
Feature 7	246.6
Feature 2	61.31
Feature 5	56.91
Feature 8	52.17
Feature 6	46.44
Feature 3	35.63

We also performed the correlation among various features, where the correlation implies the extent to which a feature might be redundant given other features. Two widely-adopted methods have been used in our experiments. First, the upper triangular of correlation matrix is carried out for discovering if a pair of strongly correlated features appear within the features, where each column in the upper triangular matrix represents the Pearson’s *r* correlation coefficient [25] of a pair of two distinct features. The Pearson’s correlation coefficient



	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	Feature 7	Feature 8
Feature 1	0.38	0.24	−0.03	−0.05	−0.03	0.39	−0.07
Feature 2		0.19	−0.02	0.14	−0.02	0.2	0.11
Feature 3			0.01	0	0.03	0.21	0.01
Feature 4				0	0.82	0.06	0.17
Feature 5					−0.02	−0.03	0.69
Feature 6						0.05	0.13
Feature 7							−0.02

FIGURE 7. Upper triangular matrix.

shows that the most of features are not strongly correlated one to each other (i.e, Pearson’s correlation coefficientj*r* j 0:9). For example, a pair of two features, Feature 1 (*The Ratio ofActive Days*) and Feature 8 (*The Percentage of Expenditure as Gifts*) represents that the highest negative correlation score is0.07 and the highest positive correlation between Feature 4 (*The Average Recharge Amount of Virtual Currency*) and Feature 6 (*The Total Amount of Expenditure*) is 0.82.

Next, we analyzed Principal Component Analysis (PCA), which can be used to evaluate variable correlation in regard to the variance of the data [26]. Figure 14 shows the experimen-tal result on PCA variables factor map [27]. In the variable factor map, each of features is expressed as an arrow and the angle between the two arrows of features implies the correlation among the respective features on the third and fourth principal components (PC). For example, given the angle between the two arrows of different two features goes near 90 degrees, they might not be correlated. As can be seen in Figure 14, the angles between the most of features are found proximate to 90 degrees (e.g., Feature 3 (The Number of Services Purchased By An Account) and Feature 5 (The Percentage of Recharge from Promotion Activities) onto the 3rd and 4th PCs), implying a weak correlation between fea-tures. According to the correlation matrix and PCA variable factor map, which show little correlation with each other, we conclude that majority of the features complement each other given their tendency towards linearly independence.

VII. CONCLUSION

This paper presents a novel system, *ProGuard,* to automati-cally detect malicious OSN accounts that participate in online promotion events. *ProGuard* leverages three categories of features including general behavior, virtual-currency collec-tion, and virtual-currency usage. Experimental results based on labelled data collected from Tencent QQ, a global lead-ing OSN company, have demonstrated the detection accu-racy of *ProGuard*, which has achieved a high detection rate of 96.67% given an extremely low false positive rate of 0.3%.

REFERENCES

[1]. Y. Wang and S. D. Mainwaring, ''Human-currency interaction: Learning from virtual currency use in China,'' in *Proc. SIGCHI Conf. HumanFactors Comput. Syst.*, 2008, pp. 25 28.

[2]. J. S. Gans and H. Halaburda, ''Some economics of private digi-tal currency,'' Rotman School Manage., Toronto, ON, Canada, Tech. Rep. 2297296, 2013.

[3]. X. Hu, J. Tang, and H. Liu, ''Online social spammer detection,'' in *Proc.28th AAAI Conf. Artif. Intell.*, 2014, pp. 59 65.

[4]. X. Hu, J. Tang, and H. Liu, ''Leveraging knowledge across media for spammer detection in microblogging,'' in *Proc. 37th Int. ACM SIGIR Conf.Res. Develop. Inf. Retr.*, 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 Trans. Depend.Sec. Comput.*, vol. 9, no. 6, pp. 811 824, Nov. 2012.

[6]. Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, ''Blog or block: Detecting blog bots through behavioral biometrics,'' *Comput. Netw.*, 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 *Proc. 21th ACMSIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2015, pp. 1769 1778.

[8]. Y.-R. Chen and H.-H. Chen, ''Opinion spammer detection in Web forum,'' in *Proc. 38th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr.*, 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 Proc. 24th ACM Int. Conf. Inf. Knowl. Manag., 2015, pp. 1601 1610.

[10]. Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, ''Twit-ter spammer detection using data stream clustering,'' Inf. Sci., vol. 260, pp. 64 73, Sep. 2014.

Authors

BAAKI DURGA SRAVANI is Pursuing M.tech(CSE) from ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY,WEST GODAVARI,AP, INDIA

Dr.P.BALA KRISHNA PRASADB.Tech, M.Tech, PhD(CSE) is working as a PROFESSOR & PRINCIPAL in ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, AP, INDIA.

Dr. GOPISETTI GURU KESAVA DASUBE(CSE), ME(CSE), PHD(CSE)PROFESSOR and HOD in the DEPARTMENT OF CSE, ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, AP, INDIA.

BAAKI DURGA SRAVANI, et. al. "Identtifying Unauthorised Account in Social Networking Online Campaigning." *IOSR Journal of Engineering (IOSRJEN)*, 10(8), 2020, pp. 25-33.