ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Review: A Ranking Fraud Detection System for Mobile Apps

Raghuveer Dagade, Prof. Lomesh Ahire

[1]Student, Dept. of M.E .Comp. Network, Nutan Maharashta Institute of Engineering and Technology, Pune, India

[2]Professor, Dept. of M.E. Comp. Network, Nutan Maharashta Institute of Engineering and Technology, Pune, India

ABSTRACT: Now a days everyone is using smart phones. There is need of various applications to be installed on smart phone. To download application smart phone user has to visit play store such as Google Play Store, Apples store etc. When user visit play store then he is able to see the various application lists. This list is built on the basis of promotion or advertisement. User doesn’t have knowledge about the application (i.e. which applications are useful or useless). So user looks at the list and downloads the applications. But sometimes it happens that the downloaded application won’t work or not useful. That means it is fraud in mobile application list. To avoid this fraud, we are making application in which we are going to list the applications. To list the application first we are going to find the active period of the application named as leading session. We are also investing the three types of evidences: Ranking based evidence, Rating based evidence and Review based evidence. Using these three evidences finally we are calculating aggregation. We evaluate our application with real world data collected form play store for long time period.

KEYWORDS:Mobile Apps, ranking fraud detection, historical ranking records, evidence aggregation, review and rating.

I. INTRODUCTION

Over the past few years the number of mobile Apps has grown at a breathtaking rate. For example, there are more than 1.6 million Apps at Google Play and Apple’s App store, as of the end of July 2015. To inspire the development of mobile Apps, poly App stores launched daily App leaderboards, which manifest the chart rankings of most popular Apps. Truly, one of the most eventful ways for mobile Apps promoting is the App leaderboard. A huge number of downloads and million dollars in revenue usually leads to a higher rank on the leaderboard. Therefore, App developers to have their Apps ranked as high as possible in App leaderboards for that they tend to explore different ways such as advertising campaigns to promote their Apps in such order.

However, as a recent trend, shady App developers resort to some fraudulent means to deliberately boost their Apps and in the end manipulate the chart rankings on an App store, instead of relying on traditional marketing solutions. This is usually implemented by using so-called “bot farms” or “human water armies” to filled the App downloads, ratings and reviews in a very short time. For example, an article from VentureBeat [4] reported that, when with the help of ranking manipulation an App was promoted, it could be propelled from number 1,800 to the top 25 in Apple’s top free leaderboard and more than 50,000-100,000 new users could be acquired within a couple of days. Indeed, the mobile App industry great concerns to such ranking fraud raises. For example, Apple has warned of cracking down on App developers who commit ranking fraud [3] in the Apple’s App store.

II. RELATED WORK

The first is about web ranking spam detection. Particularly, the web ranking spam refers to any deliberate Actions which bring to selected webpages an unjustifiable Favorable relevance or importance [3]. For example,Ntoulaset al. [3] have studied various aspects of content-based spam on the web and presented a number of heuristic methods for detecting content based spam. Zhou et al. [3] have studied the problem of unsupervised web ranking spam detection. Specifically, they proposed an efficient online link spam and term spam detection methods using spamicity. Recently, Spirin and Han [5] have reported a survey on web spam detection, which comprehensively

DOI: 10.15680/IJIRCCE.2015. 0311184

introduces the principles and algorithms in the literature. Actually, the work of web ranking spam detection is mainly based on the analysis of ranking principles of search engines, like PageRank and query term frequency. This is different from ranking fraud detection for mobile Apps.

The second category is concentrated on detecting online review spam. For example, Lim et al. [9] have identified several indicative behaviors of review spammers and model these behaviors to detect the spammers. Wu et al. [7] have studied the problem of detecting hybrid shilling attacks on rating data. The proposed approach is based on the semi supervised learning and can be used for reliable product recommendation. Xie et al. [8] have studied the problem of singleton review spam detection. Specifically, they solved this problem by detecting the co-anomaly patterns in multiple review based time series. Although some of above approaches can be used for anomaly detection from historical rating and review records, they are not able to extract fraud evidences for a given time period (i.e., leading session).

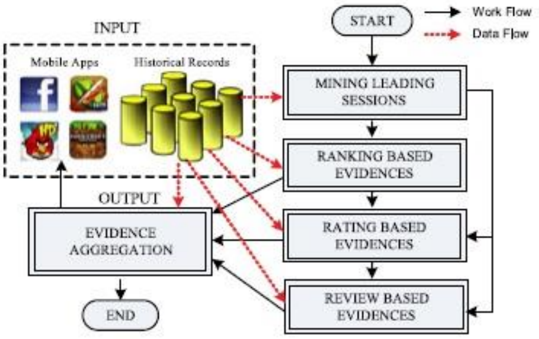
Finally, the third category includes the studies on mobile App recommendation. For example, Yan and Chen [11] developed a mobile App recommender system, named Appjoy, which is based on user's App usage records to build a preference matrix instead of using explicit user ratings. Also, to solve the sparsity problem of App usage records, Shi and Ali [4] studied several recommendation models and proposed a content based collaborative filtering model, named Eigenapp, for recommending Apps in their website Getjar. In addition, some researchers studied the problem of exploiting enriched contextual information for mobile App recommendation. For example, Zhu et al. [10] proposed a uniform framework for personalized context-aware recommendation, which can integrate both context independency and dependency assumptions. However, to the best of our knowledge, none of previous works has studied the problem of ranking fraud detection for mobile Apps.

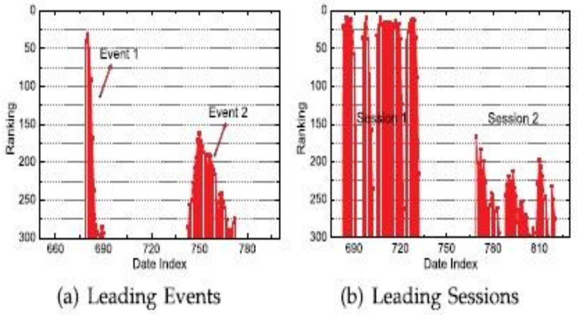
III. PROPOSED SYSTEM

Careful observation manifest that mobile Apps are not always ranked high in the leaderboard, but in some leading events, which is form different leading sessions. We can say that, ranking fraud usually happens in these leading sessions. So, detecting ranking fraud of mobile Apps is truly to detect ranking fraud within leading sessions of mobile Apps. Specifically, we first propose a simple yet convincing algorithm to identify the leading sessions of each App based on its historical ranking records. At that time, with the analysis of Apps' ranking behaviours, we find that the fraudulent Apps often have different ranking patterns in apiece leading session liken with normal Apps. Thus, we characterize some evidences which is fraud from App's historical ranking records, and develop three task to extract such ranking based fraud evidences. Nonetheless, the evidences of ranking based can be affected by App developers' reputation and some legitimate marketing campaigns, such as "limited period discount and more". As a conclusion, it is not sufficient to only use ranking based evidences. Therefore, we further suggest two types of fraud evidences based on App's review and rating history, which reflect some discrepancy patterns from Apps' historical rating and review records. Furthermore, we develop an unsupervised evidence aggregation method to merge these three types of evidences for evaluating the credibility of leading sessions from mobile Apps. Fig. 1 shows the framework of ranking fraud detection system for mobile Apps.

A. *Identifying Leading Sessions for Mobile Apps*

The App leaderboard of play storemanifest top K popular Apps with respect to various categories, such as"Top Paid Apps" and"Top Free Apps". Besides, the leaderboard is usually updated periodically (e.g., daily). So, each indivisualmobile App *a* has many historical ranking records which can be denoted as a time series, $R_a = \{r^a_1, . . . , r^a_i , . . . , r^a_n\}$, where $r^a_i \in \{1, . . .,K,+\infty\}$ is the ranking of a at time stamp t_i; $+\infty$ means a is not ranked in the top K list; n indicates the number of all ranking records. Note that, the smaller value r^a_ihas, the higher ranking position the App attains. To the analysis the historical ranking records of mobile Apps, we notice that in the leaderboardApp's are not always ranked high, nevertheless only in some leading events. For example, Fig. 2a shows an example of leading events of a mobile App. Now, we define a leading event as follows:





(a) Leading Events (b) Leading Sessions

Fig1: The framework of our ranking fraud detection system for mobile Apps.**Fig 2:** (a) Example of leading events; (b) Example of leading sessions

Note that we apply a ranking threshold* which is usually smaller than K here because K may be very big (e.g., more than 1,000), the ranking records yonder K* (e.g., 300) are not very useful for detecting the ranking manipulations.

In addition, we also notice that some Apps have several adjoining leading events which are close to each other and form a leading session. Shows a Fig. 2b, is an example of adjacent leading events of a given mobile App, which form two leading sessions. Specifically, a leading event which does not have other nearby neighbours can also be treated as a special leading session. The stately definition of leading session is as follows:

Intuitively, the leading sessions of a mobile App represent its times of popularity, therefore the ranking manipulation will only take place in these leading sessions. So, the issue of detecting ranking fraud is to detect fraudulent leading sessions. Along this line, the first job is how to mine the leading sessions of a mobile App from its historical ranking records.

A. *Extracting Evidences for Ranking Fraud Detection*

In this section, we study how to extract and merge fraud evidences for ranking fraud detection.

a. *Ranking Based Evidences*

By analysing the Apps' historical ranking records, we observe that Apps' ranking behaviours in a leading event always satisfy a particular ranking pattern, which include the three dissimilar ranking phases, namely, rising phase, maintaining phase and recession phase. Particularly, in every one leading event, an App's ranking first increases to a peak position in the leaderboard (i.e., rising phase), at that time keeps such peak position for a period (i.e., maintaining phase), and lastly lessen till the end of the event (i.e., recession phase). Fig. 3 shows an example of different ranking phases of a leading event. In addition, such a ranking pattern shows a fundamental understanding of leading event. In the following, we formally define the three ranking phases of a leading event.

b. Rating Based Evidences

For ranking fraud detection are uses the ranking based evidences. However, sometimes, it is not sufficient to only use ranking based evidences. For instance, some Apps developed by the famous developers, such as Gameloft, may have some leading events with large values of u1 due to the developers' credibility and the "word-of-mouth" advertising effect. Additionally, some of the legal marketing services, such as "limited-time discount", may also result in significant ranking based evidences. To solve that problem, we additionally study how to extract fraud evidences from Apps' historical rating records. Specifically, after an App has been published, it can be rated by any user who downloaded it. Indeed, user rating is one of the most valuable features of App advertisement. An App which has higher rating may attract more users to download and also can gives ranked higher in the leaderboard. Thus, rating manipulation is also a valuable perspective of ranking fraud. Innocently, if an App has ranking fraud in a leading session s, the ratings during the time period of s may have inconsistency patterns merged with its historical ratings, which can be used for constructing rating based evidences.

c. Review Based Evidences

In addition ratings, most of the App stores also permit users to write some textual comments as App reviews. Such reviews can indicates the individual perceptions and usage experiences of existing users for particular mobile Apps.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Indeed, review manipulation is one of the most valuable perspective of App ranking fraud. Specifically, before downloading or purchasing a new mobile App, users usually first read its historical reviews to ease their decision making, and a mobile App contains more encouraging reviews may captivate more users to download.

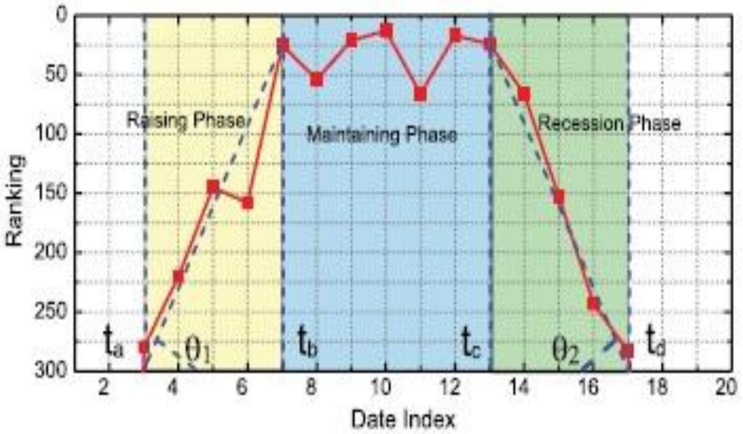


Fig 3: An example of different ranking phases of a leading event.

Therefore, imposters often post fake reviews in the leading sessions of a particular App in order to increases the App downloads, and thus propel the App's ranking position in the leaderboard.

For all that previous works on review spam detection have been reported in recent years [4], [9], the issue of detecting the local inconsistency of reviews in the leading sessions and capturing them as evidences for ranking fraud detection are still under explored. For this purpose, here we propose two fraud evidences for detecting ranking fraud based on Apps' review behaviours in leading sessions.

d. Evidence Aggregation

After extracting all three types of fraud evidences, then the next challenge is how to combine them for ranking fraud detection. In addition, there are many methods of ranking and evidence aggregation in the literature, such as permutation based models [7], [8], score based models [11], and Dempster Shafer rules [10], [12]. However, some of these methods focus on learning a global ranking for all applicants. This way is not proper for detecting ranking fraud for new Apps. Distinct methods are based on supervised learning techniques, which rely on the labelled training data and are hard to be exploited. Rather, we suggest an unsupervised approach based on fraud similarity to combine these evidences.

IV. DISCUSSION

Here, we provide some discussion about the proposed ranking fraud detection system for mobile Apps. First, the download information is an fundamental signature for detecting ranking fraud, because ranking manipulation is to use so-called "bot farms" or "human water armies" to inflate the App downloads and ratings in a very short time. However, the instant download data of each mobile App is usually not available for analysis. In fact, Apple and Google do not provide accurate download data on any App. Moreover, the App developers themselves are also reluctant to release their download data for various reasons. For that, in this paper, we mainly focus on extracting evidences from Apps' historical ranking, review and rating records for ranking fraud detection. But, our approach is scalable for merging other evidences if obtainable, such as the evidences depends on the download data and App developers' reputation.

Second, the proposed approach can discover ranking fraud happened in Apps' historical leading sessions. Nevertheless, sometime, we require to detect such ranking fraud from Apps' present ranking observations. Actually, given the current rankingr^a_{now} of an App **a**, we can detect ranking fraud for itin two distinct cases. First, if r^a_{now}> K^*, where K^* is the ranking threshold, we believe adoes not include in ranking fraud, then thisis not in a leadingevent. Second, if r^a_{now}< K^*, which means **a** is in a new leading event **e**, we behave this case as a special case thatt^e_{end}=t^e_{now} and θ_2= 0. So, such real time ranking frauds also can be discovered by the proposed approach.

Finally, after detecting ranking fraud for each and every leading session of a mobile App, the remainder issue is how to estimate the credibility of this App. In addition, our approach can detect the local anomaly instead of the global anomaly of mobile Apps.

V. EXPERIMENTAL RESULT

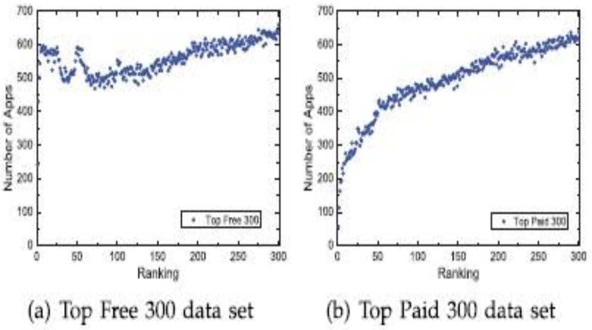
In this section, we evaluate the performances of ranking fraud detection using real-world App data.

A. *The Experimental Data*

The experimental data sets were collected from the “Top Free 300” and “Top Paid 300” leaderboards of Apple’s App Store (U.S.) from February 2, 2010 to September 17, 2012. The data sets contain the daily chart rankings1 of top 300 free Apps and top 300 paid Apps, respectively. Furthermore, each data set also contains the user ratings and review information. Figs. 5a and 5b indicates the distributions of the number of Apps with respect to different rankings in these data sets. In these figures, we can notice that the number of Apps with low rankings is more than that of Apps with high rankings. Additionally, the competition between free Apps is more than that between paid Apps, especially in high rankings (e.g., top 25). Figs. 6a and 6b show the distribution of the number of Apps with respect to different number of ratings in these data sets. In these figures, we can notice that the distribution of App ratings is not even, which shows that only a small percentage of Apps are very popular.

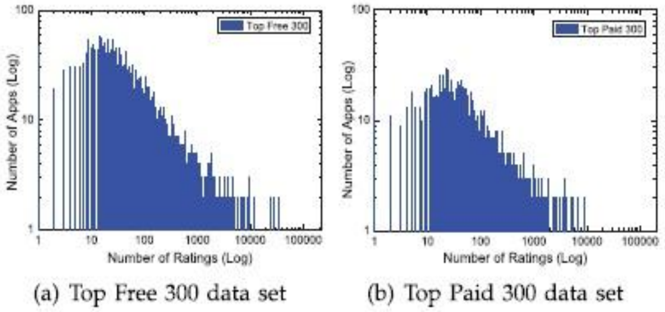
B. *Mining Leading Sessions*

Here, we indicate the results of mining leading sessions in both data sets. Specifically, in Algorithm 1, we set the ranking threshold k* = 300 and threshold ϕ = 7. This denotes two adjacent leading events can be segmented into the same leading session if they happen within one week of each other. Figs. 7 and 8 show the distributions of the number of Apps with respect to different numbers of contained leading events and leading sessions in both data sets. In these figures, we can notice that only a few Apps have many leading events and leading sessions. The average numbers of leading events and leading sessions are 2:69 and 1:57 for free Apps, and 4:20 and 1:86 for paid Apps. Moreover, Figs. 9a and 9b show the distribution of the number of leading sessions with respect to different numbers of contained leading events in both data sets. In the figures, we can find only a few leading sessions contain many leading events.



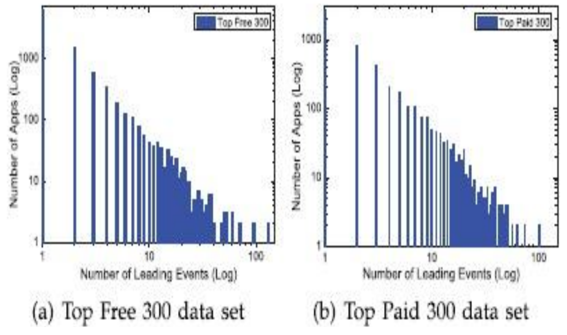
(a) Top Free 300 data set (b) Top Paid 300 data set

Fig 5: The distribution of the number of Apps w.r.t different rankings.



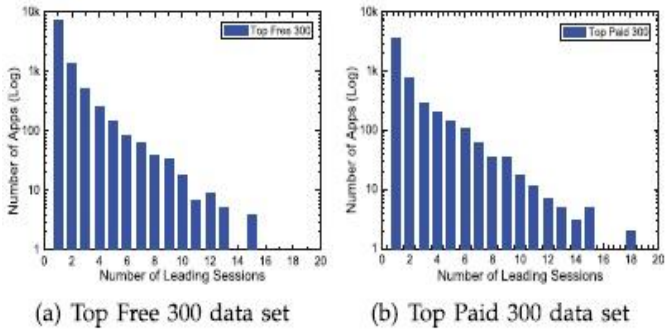
(a) Top Free 300 data set (b) Top Paid 300 data set

Fig 6: The distribution of the number of Apps w.r.t different numbers of ratings.



(a) Top Free 300 data set (b) Top Paid 300 data set

Fig. 7. The distribution of the number of Apps w.r.t different numbers Of ratings.



(a) Top Free 300 data set (b) Top Paid 300 data set

Figure 8: The distribution of the number of Apps w.r.t different number of leading sessions.

VI. CONCLUSION AND FUTURE WORK

We conclude that, to develop a ranking fraud detection system for mobile Apps. we first discover that ranking fraud occur in leading sessions and provided a method for mining leading sessions for each App from its historical ranking records. In that case, we identified ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud. Furthermore, we proposed an optimization based aggregation method to integrate all the evidences for evaluating the reliability of leading sessions from mobile Apps. That all the evidences can be modelled by statistical hypothesis tests for the unique perspective of this approach, thus it is easy to be extended with other evidences from domain knowledge to detect ranking fraud. Ultimately, we validate the proposed system with extensive experiments on real world App data collected from the google play store. Experimental results showed the effectiveness of the proposed approach.

REFERENCES

[1] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly, "Detecting spam web pages through content analysis," in Proc. 15th Int. Conf. World Wide Web, 2006, pp. 83-92.K.

[2] N. Spirin and J. Han, "Survey on web spam detection: Principles and algorithms," SIGKDD Explor. Newslett., vol. 13, no. 2, pp. 50-64, May 2012.

[3] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc. 19thACMInt. Conf. Inform. Knowl. Manage., 2010, pp. 939–948.

[4] K. Shi and K. Ali, "Getjar mobile application recommendations with very sparse datasets," in Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2012, pp. 204–212.N.

[5] Z. Wu, J. Wu, J. Cao, and D. Tao, "HySAD: A semi-supervised hybrid shilling attack detector for trustworthy product recommendation," in Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2012, pp. 985–993.

[6] S. Xie, G. Wang, S. Lin, and P. S. Yu, "Review spam detection via temporal pattern discovery," in Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2012, pp. 823–831.

[7] B. Yan and G. Chen, "AppJoy: Personalized mobile application discovery," in Proc. 9th Int. Conf. Mobile Syst., Appl., Serv., 2011, pp. 113–126.

[8] H. Zhu, H. Cao, E. Chen, H. Xiong, and J. Tian, "Exploiting enriched contextual information for mobile app classification," in Proc. 21stACMInt. Conf. Inform. Knowl. Manage., 2012, pp. 1617–1621.

[9] H. Zhu, E. Chen, K. Yu, H. Cao, H. Xiong, and J. Tian, "Mining personal context-aware preferences for mobile users," in Proc. IEEE 12th Int. Conf. Data Mining, 2012, pp. 1212–1217.

[10] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Ranking fraud detection for mobile apps: A holistic view," in Proc.

[11] 2014). [Online]. Available: http://en.wikipedia.org/wiki/cohen's_kappa

[12] (2014). [Online]. Available: http://en.wikipedia.org/wiki/information_retrieval

DOI: 10.15680/IJIRCCE.2015. 0311184