AN ENHANCED MINING LEADING SESSION ALGORITHM FOR
FRAUD APP DETECTION IN MOBILE APPLICATIONS
Javvaji Venkataramaiah, Bommavaram Sushen, Mano. R, Dr. Gladis pushpa Rathi

ABSTRACT:
Now days, mobile App is a very popular and well known concept due to the rapid advancement in the mobile technology and mobile devices. Due to the large number of mobile Apps, ranking fraud is the key challenge in front of the mobile App market. Ranking fraud refers to fraudulent or vulnerable activities which have a purpose of bumping up the Apps in the popularity list. In fact, it becomes more and more frequent for App developers to use tricky means, like increasing their Apps’ sales or posting fake App ratings, to commit ranking fraud. While the importance and necessity of preventing ranking fraud has been widely recognized. After understanding the details of ranking fraud and the need of ranking fraud detection, the paper proposes a ranking fraud detection system for mobile Apps.
The proposed system mines the active periods such as leading sessions of mobile apps to accurately locate the ranking fraud. These leading sessions can be useful for detecting the local anomaly instead of global anomaly of App rankings. Besides this, by modeling Apps ranking, rating and review behaviors using statistical hypotheses tests, we investigate three types of evidences, they are ranking based evidences, rating based evidences and review based evidences. Furthermore, we propose an aggregation method based on optimization to integrate all the evidences for fraud detection. Finally, the proposed system will be evaluated with real-world App data which is to be collected from the App Store for a long time period.

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

INTRODUCTION
The number of mobile Apps has grown up on a very large scale over the past few years. Such as, there are more than 1.6 million Apps at Apple’s App store and Google Play at the end of April 2013. To inspire the development of mobile Apps, many App stores launched daily App leader board, which shows the chart rankings of most popular Apps. This type of apps is the most important ways for promoting mobile Apps. A top rank on the leader board usually leads to a huge number of downloads and million dollars in revenue. As a result, App developers incline to explore various ways such as advertisement drive to promote their Apps to get higher position in such App leaderboards.
The recent trend in market used by the dishonest App developers for App boosting is to use fraudulent means to consciously boost their apps. At last, they also distort the chart rankings on a App store. This is usually implemented by using so-called “internet bots” or “human water armies” to raise the App downloads, ratings and reviews in a very little time. For example, Venture Beat [1] reported that, when an App was promoted using ranking manipulation, it could be precipitated from number 1,800 to the upmost 25 in Apple’s top free leaderboard and more than 50,000-100,000 new users could be acquired within a couple of days. In actuality, such ranking fraud promotes great concerns to the mobile App industry. For example, Apple has notified of cracking down on App developers who commit ranking fraud [2] in the App store.
Leading events of mobile Apps forms different leading sessions. The mobile Apps not always ranked high in the leaderboards, but it usually happens in the leading sessions. So, detecting ranking fraud of mob Apps is actually the process to detect it within the leading session of the mobile Apps. Especially, this paper proposes a simple and effective algorithm to recognize the leading sessions of each mobile App based on its historical ranking records. This is one of the fraud evidence. Also, two types of fraud evidences are proposed based on Apps’ rating and review history, which gives some anomaly patterns from Apps’ historical rating and review records. In addition, we propose an unsupervised evidence- aggregation method to consolidate these three types of evidences for assessing the credibility of leading sessions from mobile Apps.

The rest of the paper is arranged as follows: Section II presents the Existing system. In section III, proposed system is presented. Finally, the section IV concludes the review paper.

EXISTING SYSTEM
The number of mobile Apps has grown at a breathtaking rate over the past few years. For example, as of the end of April 2016, there are more than 3.6 million Apps at Apple’s App store and Google Play. To stimulate the development of mobile Apps, many App stores launched daily App leader boards, which demonstrate the chart rankings of most popular Apps. Indeed, the App leader board is one of the most important ways for promoting mobile Apps. A higher rank on the leader board usually leads to a huge number of downloads and million dollars in revenue. Therefore, App developers tend to explore various ways such as advertising campaigns to promote their Apps in order to have their Apps ranked as high as possible in such App leader boards.

Disadvantage
- They Allow Fake Application also.
- User not understanding the Fake Apps then the user also give the reviews in the fake application.
- Exact Review or Ratings or Ranking Percentage are not correctly Calculated.

PROPOSED SYSTEM
With the increase in the number of web Apps, to detect the fraudulent Apps, we have propose a simple and effective algorithm which identifies the leading sessions of each App based on its historical ranking of records. By analysing the ranking behaviours of Apps, we discover that the fraudulent Apps often have different ranking patterns in each leading session compared with normal Apps. Thus, we identify some fraud evidences from Apps’ historical ranking records and develop three functions to obtain such ranking based fraud evidences.
Further, we propose two types of fraud evidences based on Apps’ rating and review history. It reflects some anomaly patterns from Apps’ historical rating and review records. Fig. 1 shows the framework of our ranking fraud detection system for mobile Apps.

The leading sessions of mobile App signify the period of popularity, and so these leading sessions will comprise of ranking manipulation only. Hence, the issue of identifying ranking fraud is to identify vulnerable leading sessions. Along with this, the main task is to extract the leading sessions of a mobile App from its historical ranking records.

There are two main phases for detecting the ranking fraud:

i) Identifying the leading sessions for mobile apps.

ii) Identifying evidences for ranking fraud detection.

A. Identifying the leading sessions for mobile apps

Primarily, mining leading sessions has two types of steps concerning with mobile fraud apps. First, from the Apps historical ranking records, discovery of leading events is done and then second merging of adjacent leading events is done which appeared for constructing leading sessions. Certainly, some specific algorithm is demonstrated from the pseudo code of mining sessions of given mobile App and that algorithm is able to identify the certain leading events and sessions by scanning historical records one by one.

B. Identifying evidences for ranking fraud detection

1) Ranking based evidences:

It concludes that leading session comprises of various leading events. Hence by analysis of basic behaviour of leading events for finding fraud evidences and also for the app historical ranking records, it is been observed that a specific ranking pattern is always satisfied by app ranking behaviour in a leading event.

2) Rating based evidences:

Previous ranking based evidences are useful for detection purpose but it is not sufficient. Resolving the “restrict time depletion” problem, fraud evidences recognition is planned due to app historical rating records. As we know that rating is been done after downloading it by the user, and if the rating is high in leaderboard considerably that is
attracted by most of the mobile app users. Spontaneously, the ratings during the leading session gives rise to the anomaly pattern which happens during rating fraud. These historical records can be used for developing rating based evidences.

3) Review based evidences:
We are familiar with the review which contains some textual comments as reviews by app user and before downloading or using the app user mostly prefer to refer the reviews given by most of the users. Therefore, although due to some previous works on review spam detection [13] there still issue on locating the local anomaly of reviews in leading sessions. So based on apps review behaviors, fraud evidences are used to detect the ranking fraud in Mobile App.

These three evidences will be integrated by an unsupervised evidence-aggregation method for evaluating the credibility of leading sessions from mobile Apps. The statistical hypotheses tests models Apps’ ranking, rating and review behaviors to extract all the evidences. The ranking fraud detection framework is scalable and can be extended with other domain generated evidences for ranking fraud detection. Finally, we will evaluate the proposed system with real-world App data collected from the Apple’s App store for a long time span, i.e., more than two years

**DATAFLOW DIAGRAM**
**ALGORITHM**

**Mining Leading Sessions:**

There are two main steps for mining leading sessions. First, we need to discover leading events from the Apps historical ranking records. Second, we need to merge adjacent leading events for constructing leading sessions. Specifically, Algorithm 1 demonstrates the pseudo code of mining leading sessions for a given App $a$.

---

**Algorithm 1 Mining Leading Sessions**

1. $E_a = \emptyset$; $e = \emptyset$; $s = 0$; $t_{\text{start}} = 0$;
2. for each $i \in [1, |R_a|]$ do
3. if $e_i^a \leq K^*$ and $t_{\text{start}} == 0$ then
4. $t_{\text{start}} = t_i$;
5. else if $e_i^a > K^*$ and $t_{\text{start}} \neq 0$ then
6. // found one event;
7. $t_{\text{end}} = t_{i-1}$; $e = \langle t_{\text{start}}, t_{\text{end}} \rangle$;
8. if $E_a = \emptyset$ then
9. $E_a \cup e^a$; $t_{\text{start}} = t_{\text{start}}^e$; $t_{\text{end}} = t_{\text{end}}^e$;
10. else if $(t_{\text{start}} - t_{\text{end}}) < 0$ then
11. $E_a \cup e^a$; $t_{\text{end}} = t_{\text{end}}^e$;
12. else then
13. // found one session;
14. $s = \langle t_{\text{start}}, t_{\text{end}}^e, E_a \rangle$;
15. $S_a \cup s$; $s = \emptyset$ is a new session;
16. $E_a = \{e\}$; $t_{\text{start}} = t_{\text{start}}^e$; $t_{\text{end}} = t_{\text{end}}^e$;
17. $t_{\text{start}} = 0$; $e = \emptyset$ is a new leading event;
18. return $S_a$

---

**Advantages:**

- They Allow Fake Application But User See the Status of the Application and they know the application is Fake.
- The User Give the Review or Rating or Ranking are Correctly Calculated So, the Application is worth or not.

---

**CONCLUSION**

This paper reviews various existing methods used for web spam detection, which is related to the ranking fraud for mobile Apps. Also, we have seen references for online review spam detection and mobile App recommendation.

By mining the leading sessions of mobile Apps, we aim to locate the ranking fraud. The leading sessions works for detecting the local anomaly of App rankings. The system aims to
detect the ranking frauds based on three types of evidences, such as ranking based evidences, rating based evidences and review based evidences. Further, an optimization based aggregation method combines all the three evidences to detect the fraud.

REFERENCES
5. 64, May 2012.