

## FRUAD DETECTION OF MOBILE APPS

Shyamala Putti, Vidya Podugu, R.Kiran Franklin

*P.Shyamala (CSE,CMR Technical Campus)*

*P.Vidya(CSE,CMR Technical Campus)*

*R.Kiran Franklin(CSE,CMR Technical Campus)*

---

### Abstract –

These days everyone is using smart phones. There is necessity 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. Mobile App is a very popular and well known concept due to the rapid advertisement in the mobile technology and mobile devices. When user go to the play store then he is see the various application lists. This list is built on the basis of advertisement. Usually user doesn't have enough information about the application (i.e. which applications are useful or not). Then user see that list and downloads the applications. But sometimes that the downloaded application not useful. That means it is fraud in mobile application list. To avoid this fraud, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps.

**Key Words:** mining leading sessions, ranking, rating, review based evidences.

### 1.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 stimulate the development of mobile Apps, many App stores launched daily App leaderboards, which demonstrate the chart rankings of most popular Apps. 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, VentureBeat [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. The quantity of mobile Apps has developed at an amazing rate in the course of recent years. For instances, the growth of apps were increased by 1.6 million at Apple's App store and Google Play. To increase the development of mobile Apps, many App stores launched daily App leader boards, which demonstrate the chart rankings of most popular Apps and adds more ads in their app to earn. Indeed, the App leader board and mobile ads are one of the most important ways for promoting mobile Apps and for earning respectively. A higher rank on the leader board usually leads to a huge number of downloads and million dollars in revenue with mobile ads. 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 and likewise can earn more by showing multiple ads. However, as a recent trend, instead of relying on traditional marketing solutions, shady App developers resort to some fraudulent means to deliberately boost their Apps and eventually manipulate the chart rankings on an App store...

### 2. Body of Paper

We are developing a ranking fraud detection system for mobile Apps. Specifically, we first showed that ranking fraud happened in leading sessions and provided method for mining leading sessions for each App from its historical ranking records. Then, we identified ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud by using Mining Leading Sessions.

#### 2.1 Mining Leading Sessions:

In the first module, we develop our system environment with the details of App like an app store. Intuitively, the leading sessions of a mobile App represent its periods of popularity, so the ranking manipulation will only take place in these leading sessions. Therefore, the problem of detecting ranking fraud is to detect fraudulent leading sessions. Along this line, the first task is how to mine the leading sessions of a mobile App from its historical ranking records. 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.

#### 2.2 Ranking Based Evidences:

In this module, we develop Ranking based Evidences system. By analyzing the Apps historical ranking records, we serve that Apps ranking behaviors in a leading event always satisfy a specific ranking pattern, which consists of three different ranking phases, namely, rising phase, maintaining phase and recession phase. Specifically, in each leading event, an Apps ranking first increases to a peak position in the leader-board (i.e., rising phase), then keeps such peak position for a period (i.e., maintaining phase), and finally decreases till the end of the event (i.e., recession phase).

#### 2.3 Rating Based Evidences:

In the third module, we enhance the system with Rating based evidences module. The ranking based evidences are useful for ranking fraud detection. However, some-times, it is not sufficient to only use ranking based evidences. For example, some Apps created 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. Moreover, some of the legal marketing services, such as limited-time discount, may also result in

significant ranking based evidences. To solve this issue, we also study how to extract fraud evidences from Apps historical rating records.

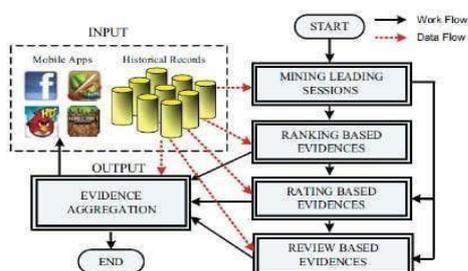


Fig-1: System Architecture

### 2.4 Review Based Evidences:

In this module we add the Review based Evidences module in our system. Besides ratings, most of the App stores also allow users to write some textual comments as App reviews. Such reviews can reflect the personal perceptions and usage experiences of existing users for particular mobile Apps. Indeed, review manipulation is one of the 16

most important perspective of App ranking fraud. Specifically, before downloading or purchasing a new mobile App, users often first read its historical reviews to ease their decision making, and a mobile App contains more positive reviews may attract more users to download. Therefore, imposters often post fake reviews in the leading sessions of a specific App in order to inflate the App downloads, and thus propel the Apps ranking position in the leader board.

### 2.5 Evidence Aggregation:

In this module we develop the Evidence Aggregation module to our system. After extracting three types of fraud evidences, the next challenge is how to combine them for ranking fraud detection. Indeed, there are many ranking and evidence aggregation methods in the literature, such as permutation based models score based models and Dempster-Shafer rules. However, some of these methods focus on learning a global ranking for all candidates. This is not proper for detecting ranking fraud for new Apps. Other methods are based on supervised learning techniques, which depend on the labeled training data and are hard to be exploited. Instead, we propose an unsupervised approach based on fraud similarity to combine these evidences

### 3. CONCLUSION

We developed a fraud detection system for mobile Apps. Specifically, we first showed that ranking fraud happened in leading sessions and provided a method for mining leading sessions for each App from its historical ranking records. Then, we identified ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud. Moreover, we proposed an optimization based on admin verification method for evaluating the credibility of leading sessions from mobile Apps. A unique perspective of this approach is that all the evidences can be model by statistical hypothesis tests, thus it is easy to be extended with other evidences from domain knowledge to detect ranking fraud. The admin can detect the ranking fraud for mobile application. The Review or Rating or Ranking given by users is correctly calculated. Hence, a new user who wants to download an app for some purpose can get clear view about the available applications. Finally; we validate the proposed system with extensive experiments on real-world App data collected from the App store. Experimental results showed the effectiveness of the proposed approach. In the future, we plan to study more effective fraud evidences and analyze the latent relationship among rating, review and rankings. Moreover, we will extend our ranking fraud detection approach with other mobile App related services, such as mobile Apps recommendation, for enhancing user experience.

### ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express my profound gratitude and deep regard to my guide **J.Srividya**, Assistant Professor for her exemplary guidance, monitoring and constant encouragement through out the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark. We also take this opportunity to express a deep sense of gratitude to Project Review Committee (PRC) **Mr. A. Uday Kiran, Mr. J. Narasimha Rao, Dr. T.S. Mastan Rao, Mrs. G. Latha, Mr. A. Kiran Kumar**, for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju**, Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy**, Director for being cooperative throughout the course of this project. We also express our sincere gratitude to **Sri. Ch. Gopal Reddy**, Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

## REFERENCES

1. (2012).[Online].Available:<http://venturebeat.com/2012/07/03/applescrackdown-on-appranki-manipulation/>
2. N. Spirin and J. Han. Survey on web spam detection: principles and algorithms. SIGKDD Explor. Newsl., 13(2):50–64, May 2012.
3. [3]<https://developer.apple.com/news/index.php?id=02062012a>.
4. E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw. Detecting product review spammers using rating behaviors. In Proceedings of the 19th ACM international conference on Information and knowledge management, CIKM '10, pages 939–948, 2010.
5. M. N. Volkovs and R. S. Zemel. A flexible generative model for preference aggregation. In Proceedings of the 21st international conference on World Wide Web, WWW '12, pages 479–488, 2012.
6. B. Zhou, J. Pei, and Z. Tang. A spamicity approach to web spam detection. In Proceedings of the 2008 SIAM International Conference on Data Mining, SDM'08, pages 277–288, 2008.
7. E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw. Detecting product review spammers using rating behaviors. In Proceedings of the 19th ACM international conference on Information and knowledge management, CIKM '10, pages 939–948, 2010.
8. Z. Wu, J. Wu, J. Cao, and D. Tao. Hysad: a semisupervised hybrid shilling attack detector for trustworthy product recommendation. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '12, pages 985–993, 2012.
9. S. Xie, G. Wang, S. Lin, and P. S. Yu. Review spam detection via temporal pattern discovery. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '12, pages 823–831, 2012.