Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

# Discovery of Ranking Fraud for Mobile Applications

[1] G Siva Manikanta, [2] Mrs. Shrija Madhu
[1] PG Student, [2]Associate Professor
[1,2]Department of Computer Applications, Godavari Institute of Engineering and Technology, Rajahmundry, India

***Abstract*—** Ranking fraud in the mobile App market refers to fraudulent or misleading tricks which have a purpose of bumping up the Apps in the status list. Indeed, it becomes more and more frequent for App developers to use shady means, such as inflating their Apps' sales or posting phony App ratings, to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized, there is limited understanding and research in this area. To this end, in this paper, this provides a holistic view of ranking fraud and proposes a ranking fraud detection system for mobile Apps. Expressly, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, this investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps' ranking, rating and review behaviors through statistical hypotheses tests. In addition, In this propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the IOS App Store for a long time period. In the experiments, can validate the success of the planned system, and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

***Keywords*—** Mobile Apps, ranking fraud detection, evidence aggregation, historical ranking records, rating and review.

## I. INTRODUCTION

The number of mobile Apps has grown at a wonderful rate over the past few years. For example, as of the end of April 2013, there are more than 1.6 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 display 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 publicity campaigns to promote their Apps in order to have their Apps ranked as high as possible in such App leader boards. However, as a recent trend, instead of relying on traditional marketing solutions, under the trees App developer's alternative to some fraudulent means to purposely boost their Apps and eventually manipulate the chart rankings on an App store. This is usually implemented by using so called "bot farms" or "human water armies" to increase the App downloads ratings and reviews in a very short time. For example, an article from Venture Beat [1] reported that, when an App was promoted with the help of ranking manipulation, it could be propelled from number 1,800 to the top 25 in Apple's top free leader board and more than 50,000100,000 new users could be acquired within a couple of days. In fact, such ranking fraud raises great concerns to the mobile App business. For example, Apple has warned of fast down on App developers who commit ranking fraud [2] in the Apple's App store. In the literature, while there are some related work, such as web ranking spam detection [3], [4], online review spam detection , and mobile App recommendation the problem of detecting ranking fraud for mobile Apps is still under-explored. To fill this critical void, in this paper, propose to develop a ranking fraud detection system for mobile Apps. Along this line, purpose of identify several important challenges.

First, ranking fraud does not always happen in the whole life cycle of an App, so In this need to detect the time when fraud happens. Such challenge can be regarded as detecting the local anomaly instead of global anomaly of mobile Apps. Second, due to the huge number of mobile Apps, it is hard to manually label ranking fraud for each App, so it is important to have a scalable way to automatically detect ranking fraud without using any standard information. Finally, due to the dynamic nature of chart rankings, it is not easy to identify and confirm the evidences linked to ranking fraud, which motivates us to discover some understood fraud pattern of mobile Apps as evidences. Indeed, our careful observation reveals that mobile Apps are not always ranked high in the leaderboard, but only in some leading events, which form different leading sessions. Note that can will introduce both leading events and leading sessions in detail later. In other words, ranking fraud usually happens in these leading sessions. Therefore, detecting ranking fraud of mobile Apps is actually to detect ranking fraud within leading sessions of mobile Apps. Specifically, In this first propose a simple yet successful algorithm to identify the leading sessions of each App based on its historical ranking records. Then, with the study of Apps' ranking behaviors, this find that the fraudulent Apps often have different ranking patterns in each leading session compared with normal Apps. Thus, the purpose of characterize some fraud evidences from Apps' historical ranking records, and develop three functions to extract such ranking based fraud evidences. Nonetheless, the ranking based evidences can be affected by App developers' status and some legitimate marketing campaigns, such as "limited-time discount". As a result, it is not sufficient to only use ranking based evidences. Therefore, in this further propose two types of fraud evidences based on Apps' rating and review history, which reflect some difference patterns from Apps' historical rating and review records.

In addition, this develops an invalid evidence-aggregation method to integrate these three types of evidences for evaluating the standing of leading sessions from mobile Apps. Fig. 1 shows the framework of our ranking fraud detection system for mobile Apps. It is importance noting that all the evidences are extracted by modeling Apps' ranking, rating and review behaviors through statistical hypotheses tests. The proposed framework is scalable and can be extended with other domain generated evidences for ranking fraud finding. Finally, In this evaluate the proposed system with real world App data collected from the Apple's App store for a long time period, i.e., more than two years. Experimental results show the effectiveness of the proposed system, the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

*Overview:* The rest of this paper is organized as follows. In Section 2, this introduces some preliminaries and how to mine leading sessions for mobile Apps. Section 3 presents how to extract ranking, rating and review based evidences and combine them for ranking fraud detection. In Section 4 this make some further discussion about the proposed approach. In section 5 purpose of report the experimental results on two long-term real-world data sets. Section 6 provides a brief review of related works. Finally, in Section 7, this concludes the paper and proposes some future research directions.

Millions of mobile Apps has grown at a huge rate over the past few years. Many App stores launched daily App leaderboards, which demo the rankings of most popular Apps. A higher rank on the leaderboard usually leads to a huge number of downloads and million dollars in revenue, in its place of relying on usual marketing solutions. Some App developers resort to some fake means to intentionally boost their Apps and eventually control the chart rankings on an App store. This is usually implemented by using so called "bot farms‖ or ―human water armies‖ to increase the App downloads, rating and reviews in a very short time. Some algorithms are available for detecting risky mobile apps such as Stateless model checking of Event-Drive application, viceroy algorithm but they are not too effective to solve a problem. Algorithm for detecting of fraud in android apps is available for example mining leading sessions but they only detect some fraudulent actions.

## II. RELATED WORK

This paper aims to identify users generating spam reviews or review spammers. In this identify several feature behaviors of review spammers and model these behaviors so as to detect the spammers. In particular, this seeks to model the next behaviors.

First, spammers may target exact products or product groups in order to maximize their impact. Second, they be likely to turn from the other reviewer in their ratings of products. In this propose scoring methods to measure the level of spam for each reviewer and apply them on an Amazon review dataset. Know then select a sub-set of highly doubtful reviewers for further scrutiny by our user evaluators with the help of a web based spammer valuation software specially developed for user evaluation experiments. Our results show that our proposed ranking and supervised methods are useful in discovering spammer smooth break other baseline method based on helpfulness votes alone. In this finally show that the detected spammers have more important impact on ratings compared with the unsupportive reviewers. From this paper be have referred:- • Concept of extracting of rating and ranking. • Concept of extracting of review[1]. Advances in GPS tracking technology have enabled us to install GPS tracking devices in city taxis to collect a large amount of GPS traces under operational time constraints. These GPS traces provide unparalleled opportunities for us to uncover taxi driving fraud activities. In this paper, be develop a taxi driving fraud detection system, which is able to systematically investigate taxi driving fraud. In this system, propese first provide functions to find two aspects of evidences: travel route evidence and driving distance evidence. Furthermore, a third gathering is designed to unite the two aspects of evidences based on dempster-Shafer theory. To implement the system, In this first identify interesting sites from a large amount of taxi GPS logs. Then, this propose a parameter-free method to mine the travel route evidences. Also, In this introduce route mark to correspond to a typical driving path from an interesting site to another one. Based on route mark, this develop a generative statistical model to characterize the sharing of driving distance and identify the driving distance evidences. Finally, can this evaluate the taxi driving fraud detection system with large scale real-world taxi GPS logs. In the experiment, be have find out some regularity of driving fraud activities and investigate the drive of drivers to commit a driving fraud by analyzing the produced taxi fraud data. From this paper be have referred:-• Concept of fraud detection [2] Evaluative texts on the Web have become a valuable basis of opinions on products, services, events, persons, etc. Recently, many researchers have studied such opinion sources as product reviews, meeting posts, and blogs. However, existing research has been focused on organization and summary vzation of opinions using normal language processing and data mining techniques. An important subject that has been neglected so far is judgment spam or trust worthiness of online opinions. In this paper, be study this issue in the context of product reviews, which are opinion rich and are broadly used by clients and product manufacturers. In the past two years, several startup companies also appeared which collective opinions from product reviews. It is thus high time to study spam in reviews. To the best of our knowledge, there is still no published study on this topic, although Web spam and email spam have been investigated expansively. In this will see that opinion spam is somewhat different from network spam and email spam, and thus requires different detection techniques. Based on the analysis of 5.8 million reviews and 2.14 million reviewers from amazon.com, in this show that opinion spam in reviews is widespread. This paper analyzes such spam activities and presents some fresh techniques to detect them [3].

Many applications in information retrieval, ordinary language processing, data mining, and related fields need a ranking of instances with respect to specified criteria as opposed to a classification. Furthermore, for many such problems, multiple recognized ranking models have been well studied and it is attractive to join their results into a joint ranking, formalism denoted as rank aggregation. This work presents a novel invalid learning algorithm for rank aggregation (ULARA) which returns a linear mixture of the person ranking functions based on the standard of rewarding ordering agreement between the rankers. In adding to presenting ULARA, we show its success on a data union task across ad hoc retrieval systems [4].

## III. PROPOSED SYSTEM

In proposed system be overcome the drawbacks of Mining leading session algorithm which is based on ranking, review & rating. First, the download information is an main signature for detecting ranking fraud, since ranking handling is to use so-called "bot farms" or "human water armies" to increase the App download and ratings in a very short time. However, the instant download information of each mobile App does often not exist for analysis. In fact, Apple and Google do not offer correct download information on any App. Furthermore, the App developers themselves are also reluctant to release their download information for various reasons. Therefore, in this paper, the focus is on extracting evidences from Apps' historical ranking, rating and review records for ranking fraud detection. However, our approach is scalable for integrating other evidences if existing, such evidences based on the download information and App developers' status. Second, the proposed come up to can detect ranking fraud happened in A,' historical leading sessions. Ranking fraud detection in mobile apps is really to detect ranking fraud within leading session of mobile apps. Specifically we identified first leading sessions based on Apps historical ranking records. Then with the analysis of Apps‘ranking behaviours this characterized some fraud evidences from historical records. The ranking based evidences can be artificial some Apps‘developer standing and some legal marketing campaigns, such as ―limited-time discount‖. This method is not enough to detect fraudulent Apps‘ so this propose two new methods of fraud evidences based on Apps‘ historical rating and review records. Additionally, in this developed an unsupervised evidence-aggregation method to add these types of evidences

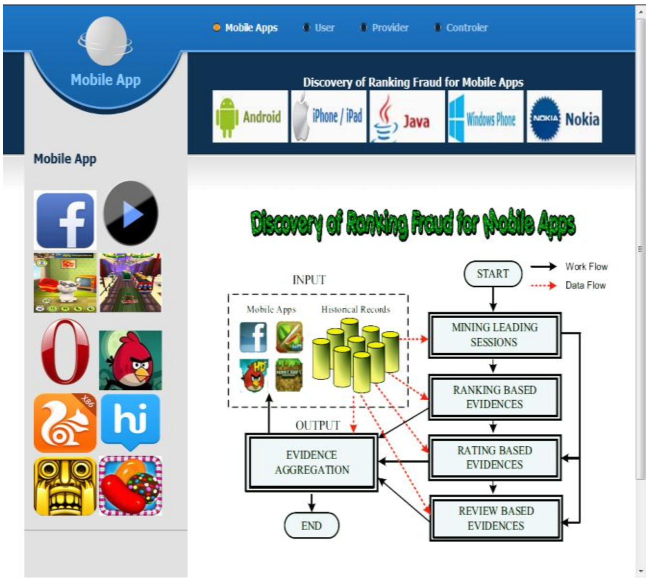
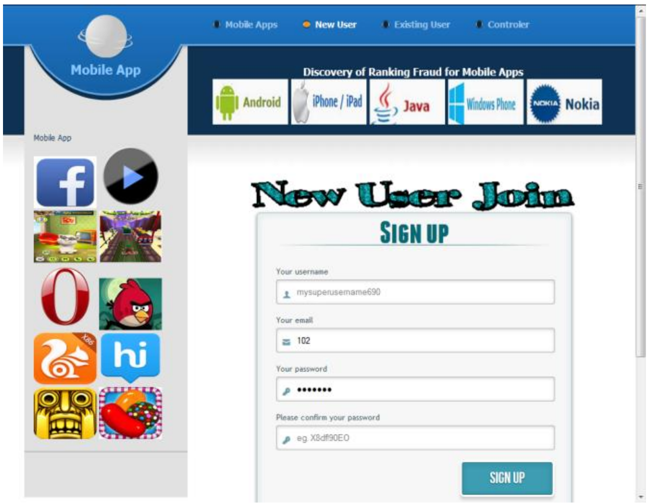


Figure 1: System Architecture

## IV. RESULT



New User Join

SIGN UP

Your username: mysuperusername690

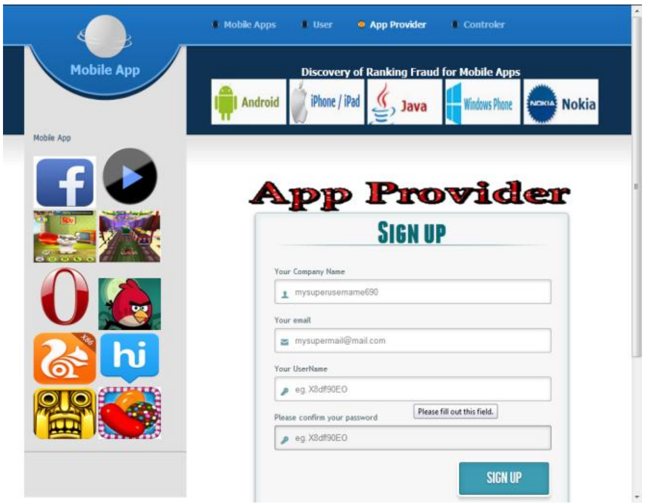
Your email: 102

Your password: •••••••

Please confirm your password: eg. X8df90EO

SIGN UP

Figure 2: New User Join Form



App Provider

SIGN UP

Your Company Name: mysuperusername690

Your email: mysupermail@mail.com

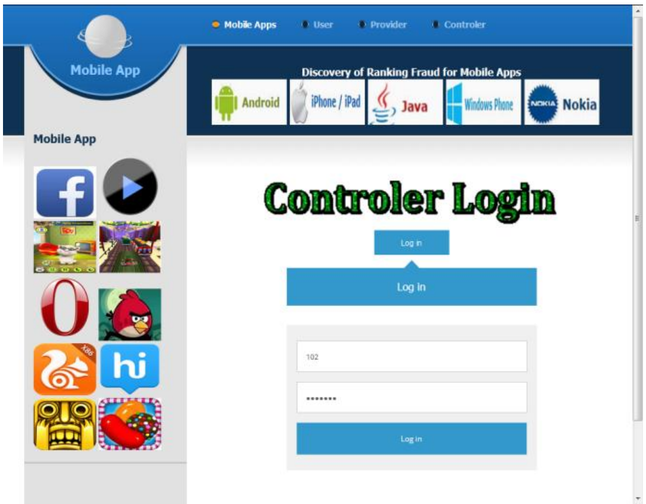
Your UserName: eg. X8df90EO

Please fill out this field.

Please confirm your password: eg. X8df90EO

SIGN UP

Figure 3: App Provider Signup Form



Controler Login

Log in

Log in

102

••••••••

Log in

Figure 4: Controller Login Form

## CONCLUSION

In this paper, developed a ranking fraud detection system for mobile Apps. Expressly, this first showed that ranking fraud happened in most main sessions and provided a method for mining leading sessions for each App from its historical ranking records. Then, we recognized ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud. Moreover, In this proposed an optimization based aggregation method to join together all the evidences for evaluating the standing of leading sessions from mobile Apps. An unique view of this approach is that all the evidences can be modeled by statistical hypothesis tests, thus it is easy to be absolute with other evidences from field knowledge to detect ranking fraud. Finally, this validate the proposed system with general experiments on real-world App data collected from the Apple’s 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 between rating, review and rankings. Moreover, In this propose will extend our ranking fraud detection approach with other mobile App related services, such as mobile Apps recommendation, for enhancing user experience.

## *References*

[1] 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.

[2] Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, “A taxi driving fraud detection system,” in Proc. IEEE 11th Int. Conf. Data Mining, 2011, pp. 181– 190.

[3] N. Jindal and B. Liu, “Opinion spam and analysis,” in Proc. Int. Conf. Web Search Data Mining, 2008, pp. 219–230.

[4] A. Klementiev, D. Roth, and K. Small, “An unsupervised learning algorithm for rank aggregation,” in Proc. 18th Eur. Conf. Mach.Learn., 2007, pp. 616–623.