

Crowdsourcing Fraud Detection Algorithm Based on Psychological Behavior Analysis

Li Peng^{1,2}, Yu Xiao-yang¹, Liu Yang², Bi Ting-ting²

1 Higher Educational Key Laboratory for Measuring and Control Technology, Instrumentations of Heilongjiang Province, Harbin University of Science and Technology, 150080 Harbin, China

2 School of Computer Science and Technology, Harbin University of Science and Technology, 150080 Harbin, China
{pli, yuxiaoyang }@hrbust.edu.cn.

Abstract. This paper present a new crowdsourcing fraud detection method based on psychological behavior analysis. We apply Ebbinghaus forgetting curve to find out the spammer according to the psychological difference between deception and reliable behavior. The experimental results show that our method is effective and feasible.

Keywords: Crowdsourcing, Ebbinghaus Forgetting Curve; Fraud Detection

1 Introduction

Crowdsourcing, a new organization form and cooperation pattern in the process of enterprise production, was grown with the rapid popularity of Internet ^[1]. Enterprises actively utilize many online user resources and allocate the outsourcing task to the interest groups by means of crowdsourcing technology, solving some limitations of traditional outsourcing service. In recent years, crowdsourcing technology has become a focus of research and researchers around the world have realized it in some practical applications. For example, Rensnik combined monolingual crowdsourcing and targeted paraphrasing to improve the quality of pure machine translation [2]; Hwang introduced mobile-based crowdsourcing into the field of environmental audio recognition, to improve the performance of mobile devices in filtering background noise ^[3]; Fritz applied crowdsourcing to global land cover, to solve the problem of ignoring potential land in statistical work ^[4]. The rapid development of crowdsourcing technology drew the Text REtrieval Conference's (TREC) attention and crowdsourcing track has attracted more than 100 groups around the world to join the competition in TREC 2013.

Unfortunately, some unreliable workers emerged due to profit driven in the practical application of crowdsourcing. Their results seriously reduce the quality and bring about the initiator's judgment biases ^[5]. Therefore, the kernel of crowdsourcing quality improvement is how to find the spammer. Fraud behavior is a kind of people's mental activity; psychological methods maybe make effective judgment on it in a

certain extent. Consequently, we put forward a crowdsourcing fraud detection method based on psychological analysis according to the psychological difference between deception and reliable behavior.

2 Behavior Analysis Based on Ebbinghaus Forgetting Curve

The German psychologist H.Ebbinghaus researched the basic rule of human memory and oblivion, and put forth "the function of time and memory" as shown in the formula (1) [6]. *OriginalLearning* stands for the number of writing from memory, when he remembered all materials in the first time. After a while, *Relearning* is the number. Thus retention scores are obtained and represented by *SavingScore*.

$$SavingScore = \frac{OriginalLearning - Re\ learning}{OriginalLearning} \times 100 \quad (1)$$

According to the formula (1), Ebbinghaus forgetting curve can be drawn (see Figure 1). In this figure, the longitudinal axis represents the memory retention scores; The horizontal axis represents elapsed time since learning. The curve conducts a quantitative expression for the forgetting rules in learning process resulting oblivion can be calculated. Human oblivion is an unbalanced development, Memory is forgotten very quickly in the initial stage, and then slows down gradually, after a certain time almost no longer forgotten.

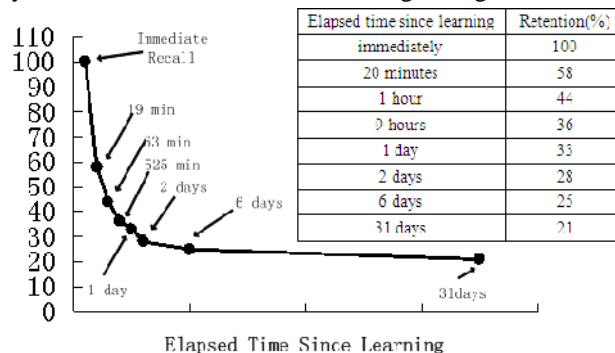


Fig. 1. Ebbinghaus forgetting curve

Fraud is usually divided into two basic types. One is random spammer, they submit results randomly and it is difficult to identify them; the other is uniform spammer, they just submit results regularly and this type is easy to be found [7]. Therefore, we only focus on the former.

The principle of our detection method is crowdsourcing participants will produce different memory rules owing to different psychological state in the process of judgment to the crowdsourcing task. Their behavior is a specific embodiment of mental activity, no matter he is a spammer or credible person. The trusted participant will strictly comply with the requirements and think hard when judging the relevance

of pairs, so It will produce a deep memory in his mind. This is the general process of human memory accord with Ebbinghaus forgetting rule. However, the spammer will only spend little or no effort on crowdsourcing and complete tasks mechanically. They lack the understanding memory about task content and their forgetting states don't comply with Ebbinghaus forgetting rule. According to above psychological differences and quantitative expression of Ebbinghaus forgetting curve, the flow chat of our algorithm is shown in Fig.2. Workers will rejudge a certain amount of repeated pairs in limited time, and then the work's SavingScore and threshold is compared, low SavingScore workers are considered as the spammer.

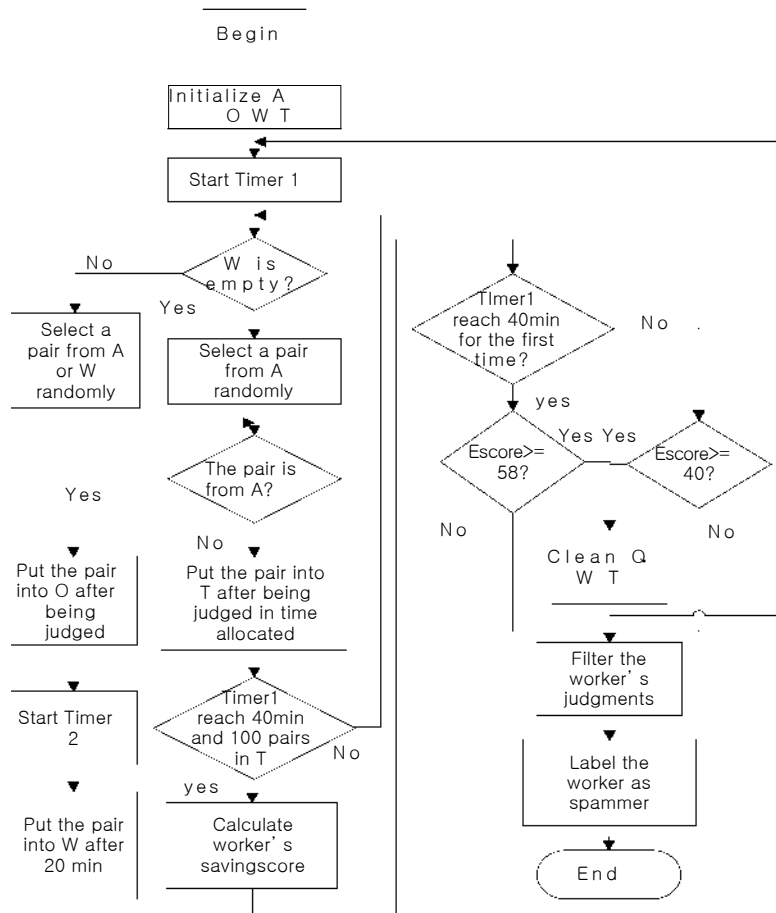


Fig. 2. The workflow of our algorithm

3 The Results and Analysis of Experiments

We constructed an online crowdsourcing experiment platform to verify the validity of our method. In the Foreign Broadcast Information Service data, a total of 1380 documents were selected from 4 themes as task document collection. All of these documents have the standard relevance labels, and contain 1120 non-relevant documents, 260 relevant documents. The experiment platform randomly assigned these tasks to 76 online students with computer background, let them label pairs.

we utilize LAM(Logistic Average Misclassification) and AUC(receiver operating characteristic curve)to evaluate the effectiveness of our method. Our method filter 13 ones from 76 workers, 11 spammers and 2 trusted workers. In addition, 3 spammers are not detected; recall and precision are 0.93 and 0.79 respectively. Final labels were selected by majority vote before and after filtration, using AUC and LAM assessed 4 topics respectively, and then assessed the whole. As a result, the overall LAM decreased by 3.7%, AUC increased by 8%.

5 Conclusion

This paper proposed an effective solving strategy on crowdsourcing fraud detection by means of psychological behavior analysis method. We creatively apply Ebbinghaus forgetting curve to find out the spammer according to the psychological difference between fraud and reliable behavior. This is an exciting exploration because we successfully applied the psychological method to the field of computer science. The experimental results show that our method is effective and feasible.

Acknowledgement. This paper is supported by National Natural Science Foundation of China (61103149) and China Postdoctoral Science Foundation (2011M500682).

References

1. Dai, Peng, Christopher, H., Daniel, S.: POMDP-based Control of Workflows for Crowdsourcing. *Artificial Intelligence*. 202, 52--85 (2013)
2. Resnik, P., Buzek, O., Kronrod, Y., Quinn, A.J., Bederson, B.B.: Using Targeted Paraphrasing and Monolingual Crowdsourcing to Improve Translation. *ACM Transactions on Intelligent Systems and Technology*. 43, 185--197 (2013)
3. Hwang, K., Lee, S.Y.: Environmental Audio Scene and Activity Recognition through Mobile-based Crowdsourcing. *IEEE Transaction on Consumer Electronics*. 582, 700--705(2012)
4. Fritz, S., McCalium, I., Schill, C., Perger, C.: Geo-wiki.org: The Use of Crowdsourcing to Improve global land cover. *Remote Sensing*. 13, 345--354(2009)
5. Zhang, Z.Q.:Research on Crowdsourcing Quality Control Strategies and Evaluation Algorithm. *Chinese Journal of Computer*. 368, 1636--1649(2013)

6. Luo, N., Yuan, F.:Detection User's Long-term Interest Based on Ebbinghaus Forgetting Curve. ICIC Express Letters, Part B: Applications. 25, 1151--1155(2011)
7. Jeroen, B.P., Arijen P.D.: Obtaining High-quality Relevance Judgments Using Crowdsourcing. 165, IEEE Internet Computing. 20--27(2012)