







USDSE: A Novel Method to Improve Service Reputation Based on Double-Side Evaluation

Jianmao Xiao¹ , Jia Zeng¹, Xu Miao², Yuanlong Cao¹ , Jing Zhao¹ ,
and Zhiyong Feng³ 

¹ School of Software, Jiangxi Normal University, Nanchang, China
{jm_xiao,ylcao}@jxnu.edu.cn, jia_zeng_jxnu@163.com, zhaojinghaze@163.com

² China Unicom Software Research Institute, Beijing, China
miaox1@chinaunicom.cn

³ College of Intelligence and Computing, Tianjin University, Tianjin, China
zyfeng@tju.edu.cn

Abstract. Fair evaluation of users is the basic guarantee for the healthy development of the service ecosystem. However, existing methods do not provide an indicator of when can get fair evaluation and how to reduce the proportion of malicious users from the root. This paper proposes a “user-service” double-side evaluation(USDSE) model to solve the problem above. Firstly, we start with getting the reputation of users by using the evaluation of service. Normal and malicious users are distinguished by their reputation. Secondly, we use the minimum number of normal users as the indicator to show when we can get fair evaluation. Finally, the revenue of employing collusive users has been analyzed to reduce the proportion of collusive users indirectly. The simulation experiments show that USDSE effectively improves the accuracy of identifying malicious users and reduces the revenue of employing collusive users.

Keywords: Evaluation of users · Evaluation of services · Reputation · Unfair rating filtering · Minimum user

1 Introduction

Evaluation of users, indicating the user’s view of the service, can reflect the quality of service. Therefore, referencing evaluations from other users to decide whether to use a particular web service has become a common method. However, for fame or interest, many service providers will employ malicious collusive users to improve their reputation or reduce the reputation of their competitors [6, 18], leading to the creation of certain blackmarket services [4], which will seriously damage the credibility of evaluation. Meanwhile, there are many unreasonable evaluations such as zombie users never evaluating services [2]; Some of the comments are fake and may not reflect spontaneous opinions [16]; irresponsible users

always give random evaluations [22]. Due to user preferences and ecosystem environmental changes, normal users may have biased judgments on the quality of services. And an online review site typically hosts millions and billions of products and ratings [19, 27]. These will make it difficult for users to find high-quality services according to the evaluation. Worse still, that will lead to the loss of users, which will damage the healthy development of the service ecosystem.

Many studies consider how to remove malicious evaluations in order to improve the fairness of user evaluations [1, 2, 5, 24] and detect fake reviews [10, 14, 16, 23]. However, there are some key limitations in the previous study.

- Many previous methods mainly collect the information from the evaluation of users [1, 24]. However, they ignore that the service itself also has a cognitive process for the user, i.e., the evaluation of service.
- Previous studies have either ignored detecting random and malicious users [11, 17] or characterized behavior malicious users too clearly [22].
- To the best of our knowledge, no indicator has been provided to show when a user can get fair evaluation [2, 17]. We hope the indicator will help users to choose the service from the evaluation at a proper time.
- Existing models fail to consider analyzing the revenue of employing malicious collusive users [22, 24]. The behavior of malicious users will also evolve as the detection mechanism changes.

In order to solve the problem mentioned above, a “user-service” double-side evaluation (USDSE) model that considers both users and services are proposed to improve the fairness of evaluation.

The main contributions of this work are listed as follows:

- By adding the evaluation of the service to the user, the double-side evaluation between the service and the user is established. USDSE effectively improves the accuracy of identifying malicious users compared with HMRep [22].
- USDSE considers multiple behaviors of malicious users. For example, malicious users may give random evaluations, malicious users may collude with each other, and service providers that employ malicious users may collude with each other to enhance their reputation.
- A proof has been given by using the Chernoff Bound and Bayes formula to get fair evaluation with minimum normal users. For cases where some malicious users are not detected or normal users mutate into malicious users, a solution has been given by taking the proportion of different user types as input.
- As far as we know, we are the first to make a revenue analysis after identifying malicious users. The experiment shows that USDSE can effectively reduce the revenue of employing collusive users and indirectly reduce the proportion of employing collusive users in the ecosystem.

2 USDSE Mechanism

2.1 Basic Framework

We envision a service ecosystem that can meet all user’s requirements. Figure 1 shows the framework of getting fair evaluation of users. In USDSE, the service

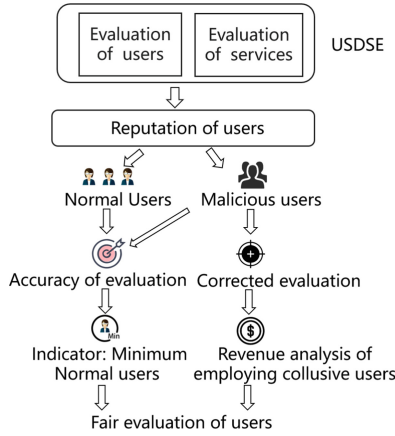


Fig. 1. Framework of getting fairness evaluation

would evaluate the user based on the user’s behavior. The user’s reputation will be calculated by the service’s evaluation of the user. Furthermore, we divide users into normal users and malicious users by their reputation. We will take the following two steps to get fair evaluation of users.

On the one hand, by using the accuracy of normal users, we can solve the problem that how many normal users are required to get fairness evaluation when a new service enters the ecosystem. On the other hand, the USDSE model will do the revenue analysis of the service providers who employ the collusive users, and compares the revenue after establishing USDSE. Intuitively, after removing the malicious user’s evaluation, the service provider’s revenue from employing collusive users will be reduced.

Figure 2 shows our user-service double-side evaluation model. The model can be divided into two parts: the evaluation of users and the evaluation of service. The user will choose the service he needs. After the service is consumed, the user reports the feedback rating regarding the level that he evaluates on the service. The service that users have evaluated would also evaluate the user in USDSE.

2.2 The Evaluation of Users

The user’s evaluation of the service reflects his satisfaction with the service, including both the satisfaction of the functional requirements and non-functional requirements, such as response time and availability. In this section, we will introduce users’ evaluation of services in USDSE.

Definition 1: For $\forall u_i \in U$, the evaluation of u_i can be defined as a tuple:

$$E_i = (WS_i, \tau_i)$$

where WS_i is the collection of services that u_i has evaluated. $WS_i = \{ws_{i1}, ws_{i2}, \dots, ws_{im}\}$, $|WS_i| = m$, m is the size of service collection; τ_i is

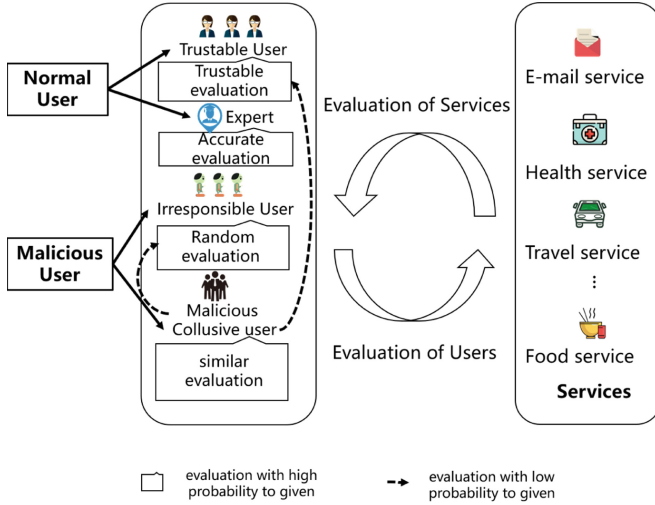


Fig. 2. Procedures of the USDSE

the function that u_i give evaluations : for $\forall ws_{ij} \in WS_i, \tau_i(ws_{ij}) = r_{ij} (r_{ij} \in [0, 5], j \in [1, m])$ r_{ij} is the feedback rating given by u_i on service ws_{ij} .

Definition 2: Users in the system can be divided into :

$$U = \{NU, MA\}$$

$NU = \{Exp, Tu\}$ is a set of experts and trustable users. $Exp = \{ex_1, ex_2, \dots, ex_p\}$, $|Exp| = p$, p is the size of experts collection, $Tu = \{tu_1, tu_2, \dots, tu_q\}$, $|Tu| = q$, q is the size of trustable users collection. $MA = \{Cou, Ir\}$ is a set of collusive users and irresponsible users. $Cou = \{cou_1, cou_2, \dots, cou_s\}$, $|Cou| = s$, s is the size of collusive users collection. $Ir = \{ir_1, ir_2, \dots, ir_t\}$, $|Ir| = t$, t is the size of irresponsible users collection. We should notice that $p + q + s + t = n$, n is the total number of users.

Definition 3: For $\forall tu_i \in Tu$, his rating function on the service can be defined as following:

$$\tau_i(ws_{ik}) = N(\mu_k, \sigma^2)$$

$N(\mu, \sigma^2)$ is a normal distribution function, where μ_k is the true quality of ws_{ik} , σ^2 represents the user's deviation on services caused by users bias.

Definition 4: For $\forall ex_i \in Ex$, his rating function on the service can be expressed as

$$\tau_i(ws_{ik}) = \mu_k$$

Definition 5: For $\forall cou_i \in Cou$, his rating function on the service can be defined as following

$$\tau_i(ws_{ik}) = f(flag_k)$$

If $flag_k = 0$ means that ws_{ik} is the service owned by employer, then $\tau_i(ws_{ik}) = highest\ score$. If $flag_k = 1$, then $\tau_i(ws_{ik}) = N(\mu_k, \sigma^2)$. It means that the collusive user will disguise as a trustable user when evaluating the current service.

Definition 6: For $\forall ir_i \in Ir$, his rating function on the service can be expressed as:

$$\tau_i(ws_{ik}) = Random(minscore, maxscore)$$

where $Random(minscore, maxscore)$ is a random function ranging from minimum score to maximum score.

2.3 The Evaluation of Services

Definition 7: The service's evaluation on the user can be modeled as a tuple:

$$SE_k = (UE_k, \zeta_k)$$

where $UE_k = \{ue_{k1}, ue_{k2}, \dots, ue_{kn}\}$ is the set of users who have evaluated the service ws_k . ζ_k is the rating function of service: for $\forall ue_{kj} \in UE_k, \zeta_k(ue_{kj}) = r_{kj}, r_{kj} \in [0, 5], j \in [1, n]$. r_{kj} means that the feedback rating on ue_{kj} given by the service ws_k .

Definition 8: For service ws_k , its evaluation function on the user can be expressed as:

$$\zeta_k(ue_{kj}) = \begin{cases} top\ score - |ws_k - \tau(ws_k)|, & T(ws_k) \geq \tau_j(ws_k) \\ top\ score, & \\ T(ws_k) < \tau_j(ws_k) & \end{cases}$$

where $\zeta_k(ue_{kj})$ is the feedback rating of u_j given by ws_k . $\tau_j(ws_k)$ is the rating given by u_j , $T(ws_k)$ is the cognitive function of the service based on its quality, and will return the true quality of the service itself. We assume that the service has a clear understanding of its own quality. If the evaluation given by the user is higher than its true quality, it will give the highest score $maxscore$ as feedback rating. If the evaluation given by the user is lower than the true quality of the service itself, the feedback ratings of the users will be determined according to the deviation between the true quality of service and the evaluation of users.

2.4 Reputation Calculation and Identification of Different Types of Users

In this section, we will introduce how to calculate the reputation of users and identify different types of users.

Definition 9: For $\forall u_i \in U$, his reputation is calculated as follows:

$$r_j^i = \left(\sum_{k=1}^m \zeta_k(ue_{kj}) \right) / m$$

$$r_j = (1 - \lambda) * r_j + (\lambda * r_j^i)$$

where r_j^i is the average reputation given by all the services which u_j has evaluated. r_j is the current reputation of u_j . λ is the learning rate which can reflect the effect of history to the reputation.

Definition 10: We can use (1) to distinguish different users.

$$g(u) = \begin{cases} Nu, & \text{if } r_j > K \\ MA, & \text{else} \end{cases} \quad (1)$$

$g(u)$ is the function to judge the types of user. When the reputation of user is greater than the specified threshold, the model considers it as a normal user. Moreover, we identify experts by the following inequality

$$r_j > T(T \geq K)$$

Definition 11: We identify collusive users through evaluation similarity clustering. The collusion detection process is as follows: Firstly, we will calculate the evaluation similarity among users in MA

$$s_{ef} = 1 - \sqrt{\frac{\sum_{i=1}^l (\tau_e(ws_{ei}) - \tau_f(ws_{fi}))^2}{(l+1)}}$$

l is the size of service collection where the service is the common service evaluated by u_e and u_f . Then we will construct the maximum spanning tree of fuzzy graph in the collection of malicious users, where V denotes the set of vertices and E denotes the set of undirected edges. The weight of an edge is the evaluation similarity of the two connected vertices calculated by the above equation. Then we will cut the edges with the weight below φ to perform clustering [22]. Moreover, remove collusive users from malicious users, the remaining users are irresponsible users.

2.5 Minimum Number of Normal Users to Get Fair Evaluation

In order to get fair evaluation, we use the minimum number of users as an indicator to show when can get fair evaluation. For a given accuracy of service evaluation A , the minimum number of normal users to get the fair evaluation can be calculated as:

$$n = \frac{-\ln(1-A) * 2 * (\theta * \alpha + \nu * (1-\alpha))}{(\theta * \alpha + \nu * (1-\alpha) - 1/2)^2} \quad (2)$$

where θ is the mean accuracy of normal users, while ν is the mean accuracy of malicious users. α is the proportion of users who will perform fair evaluation on services in the normal user. α can reflect the normal user. When α is equal to 100%, which means that we think all the normal users detected in USDSE will make the correct evaluation of the service. When α equals 10%, it means that only 90% of the normal users detected in USDSE will give the correct rating. The proof is as follows: we assume that the normal users are more likely to give a correct evaluation. p_i is the probability that u_i will give correct evaluation

of the service. Further, at least $n/2$ normal users in the system will give fair evaluation. The probability of at least $n/2$ normal users will give fair evaluation on service can be calculated as:

$$P_{\frac{n}{2}} = \sum_{\xi \subseteq U, |\xi| \geq \lceil n/2 \rceil} \prod_{u_i \in \xi} p_i \prod_{u_j \notin \xi} (1 - p_j)$$

The mean value of $P_{n/2}$ is:

$$\begin{aligned} E\left(P_{\frac{n}{2}}\right) &= E\left(\sum_{\xi \subseteq U, |\xi| \geq \lceil n/2 \rceil} \prod_{u_i \in \xi} p_i \prod_{u_j \notin \xi} (1 - p_j)\right) \\ &= E\left(\sum_{k=\lceil n/2 \rceil}^n \left(\sum_{\xi \subseteq U, |\xi|=k} \left(\prod_{u_i \in \xi} p_i \prod_{u_j \notin \xi} (1 - p_j)\right)\right)\right) \\ &= \left(\sum_{k=\lceil n/2 \rceil}^n \left(\sum_{\xi \subseteq U, |\xi|=k} \left(\prod_{u_i \in \xi} E(p_i) \prod_{u_j \notin \xi} E(1 - p_j)\right)\right)\right) \end{aligned} \tag{3}$$

We can see that $E(u_i) = \mu$, then the above user mean value is:

$$\begin{aligned} E\left(P_{\frac{n}{2}}\right) &= \left(\sum_{k=\lceil n/2 \rceil}^n \left(\sum_{\xi \subseteq U, |\xi|=k} \left(\prod_{u_i \in \xi} \mu \prod_{u_j \notin \xi} (1 - \mu)\right)\right)\right) \\ &= \left(\sum_{k=\lceil n/2 \rceil}^n \left(\sum_{\xi \subseteq U, |\xi|=k} (\mu^k (1 - \mu)^{n-k})\right)\right) \\ &= \sum_{k=\lceil n/2 \rceil}^n C_n^k \mu^k (1 - \mu)^{(n-k)} \end{aligned} \tag{4}$$

According to Chernoff bound¹,

$$\sum_{k=\lceil n/2 \rceil}^n C_n^k \mu^k (1 - \mu)^{(n-k)} \geq 1 - e^{\left(-\frac{1}{2\mu} n(\mu - 1/2)^2\right)} \tag{5}$$

In this paper, we use the average accuracy of users u_i to replace the $E(u_i)$, the following will be used to calculate μ .

$$E(u_i) = \frac{\sum_{j=1}^m \frac{r_{ij} - \bar{r}_j}{\text{Max}(\bar{r}_j - \text{minscore}, \text{maxscore} - \bar{r}_j)}}{m} \tag{6}$$

\bar{r}_j is the real quality of ws_{ij} which could be calculated using the average rating of all normal users. $\text{Max}(\bar{r}_j - \text{minscore}, \text{maxscore} - \bar{r}_j)$ is the maximum deviation between \bar{r}_j and user could give. Assume that the accuracy of the evaluation is required to be A , as long as the above formula is made larger than A . We can get minimum of users to get fair evaluation. However, the malicious user may gain trust through camouflage, and suddenly launch an attack at a certain time,

¹ https://en.wikipedia.org/wiki/Chernoff_bound.

causing damage to the credibility of the service. Therefore, we need to consider the situation in which some users suddenly become malicious collusive users. The user type in the system is $U = \{NU, MA\}$, then for the u_i , his probability of giving the fair evaluation is:

$$P(u_i) = P(\text{fair evaluation}|NU) * P(NU) + P(\text{fair evaluation}|MA) * P(MA) \quad (7)$$

when the user is normal, $E(p_N)$ is the probability that a normal user gives fair evaluation on the service; when the user is malicious, $E(p_M)$ is the probability that a malicious user gives fair evaluation on the service. Based on the historical data of the USDSE, we can see calculate that $E(p_N) = E(P(\text{fairevaluation}|NU)) = \theta$ from normal users detected in USDSE. $E(p_M) = E(P(\text{fairevaluation}|MA)) = \nu$ from malicious users. Notice that $E(P(u_i)) = \theta * \alpha + \nu * (1 - \alpha)$. Finally, the minimum number of normal user to get the fair service evaluation can be shown as (2).

2.6 Revenue Analysis of Employing Collusive Users

The basic purpose of the general service provider to employ collusive user is to improve its own revenue. Figure 3 shows two scenarios in which service providers employ collusive users. In scenario 1, service providers employ collusive users respectively to improve their reputation. In USDSE, the services provided by the service provider will also give these collusive users a good evaluation and help them improve their reputation. In scenario 2, the service providers will collaborate with others to employ collusive users, and the collusive users will evaluate all the services of these cooperative service providers. The following equation can be used to calculate the revenue of employing collusive users.

$$\begin{aligned} net_revenue &= rre - totalCost \\ rb &= \frac{1}{1 + e^{-increase_rating}} \\ totalCost &= \sum_{i=1}^{cnum} \sum_{j=1}^{en} cost_onetime + cc \\ cost_onetime &= \beta * eq (\beta > 0) \\ cc &= k * costofColluding (k > 0) \end{aligned} \quad (8)$$

The *net_revenue* is the total revenue obtained by employing collusive users. *rre* is the revenue obtained by the raise of users' evaluation with the help of collusive users. *increase_rating* is the increase of service's rating after employing malicious collusive users. *totalCost* is the total cost of employing collusive users. *cnum* is the total number of collusive users. *en* is total evaluation number for a collusive user. *cost_onetime* is the cost of one evaluation for a collusive user which depends on the quality of evaluation(*eq*). Intuitively, when the malicious user pretends to evaluate the service as normal users, the cost will increase compared with random evaluation. λ is the parameter describing the relation between the quality of evaluation and the cost at one time. *cc* is the communication

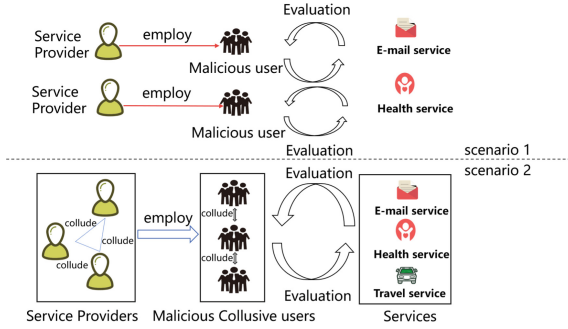


Fig. 3. Two scenarios for collusive user

cost among service providers. $costofColluding$ is the cost of colluding a service provider. k is the number of service providers who collude together to employ users.

3 Experimental Evaluation

Because of the current limited availability of evaluation data, many existing methods [15, 22, 24] used simulation data for performance evaluation. The simulated malicious and subjective evaluation can reflect the real situations by setting the magnitude (e.g. 1, 2, . . . , 10) of subjective feedback ratings and the density (e.g. 10, 20, . . . , 100%) of malicious feedback ratings [13, 22]. Hence, in our experiments, we also employ simulation to generate malicious and biased feedback ratings to evaluate the proposed approach.

3.1 Dataset

In the simulation experiment, the number of users is 1000, the number of services is 50. To evaluate our scheme’s capability of detecting malicious users, the collusive user ratio varies from 0% to 100%. For example, if the collusive user ratio is 50%, that means half of the malicious users are irresponsible and give random ratings and half of the malicious users are colluding. We simulated three scenarios in the experiment.

- 700 normal users, 300 malicious users, the percentage of normal users is high (HNU)
- 500 normal users, 500 malicious users, the percentage of normal users is medium (MNU)
- 300 normal users, 700 malicious users, the percentage of normal users is low (LNU)

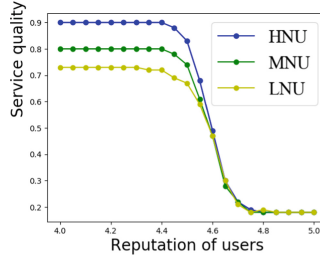


Fig. 4. F1-score in three scenarios

For simplicity, we set the ratio of trusted users to experts to be 1: 9. We use NS, CS, and IS to represent the set of normal users, collusive users, and irresponsible users, respectively, to allow DNS, DCS, and DIS to represent the set of normal users, collusive users, and irresponsible users detected in USDSE. The evaluation index is F1-Score, F1-score is the weighted sum of model precision and recall rate, taking into account the precision and recall rate of the model, as defined below:

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall}$$

$$Precision = \frac{\|DGS \cap GS\|}{(\|DGS \cap GS\| + \|DGS \cap (CS \cup IS)\|)} \quad (9)$$

$$Recall = \frac{\|DGS \cap GS\|}{(\|DGS \cap GS\| + \|(DIS \cup DIS) \cap GS\|)}$$

3.2 Studies on Parameters

The reputation of users can be obtained based on the evaluation of services. When the reputation of the user is greater than K, it is considered a normal user. In order to find a reasonable K to achieve better performance, we set the user reputation ranging from 4 to 5 and use F1-score as the evaluation index. In the above three scenarios, the ratio of the collusive user and the irresponsible user is 50% (the result is the same with the change of the ratio of collusive user ratio in HNU, MNU, LNU). Figure 4 shows the variation of F1-score in three different scenarios. When the K value is set between 4 to 4.4, F1-score is the highest, in other words, the model works best; when the K is greater than 4.4, the F1-score decreases. That is because there is a certain bias in the evaluation of the services for some normal users caused by the environment and subjective preferences.

3.3 Malicious User Detection

In order to test the effect of the USDSE mechanism to identify normal users, we compare the USDSE with HMRep [22]. HMRep uses the deviation of rating

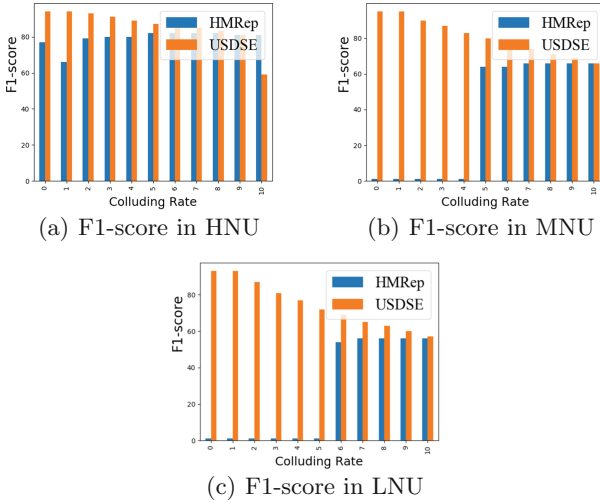


Fig. 5. F1-score compared with HMRrep

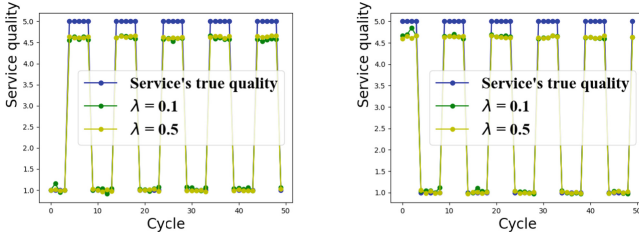
to identify different types of users. Figure 5 shows the effect of USDSE and HMRrep in three scenarios. USDSE can maintain a high F1-score value in all three scenarios, up to 95%. This is mainly due to the use of services on the evaluation of users which can better reflect the true quality of users; when the proportion of malicious users is less than 60%, USDSE is more efficient than HMRrep. This is because the proportion of irresponsible users is high and the characteristics of evaluation behavior are easy to distinguish.

3.4 Response to Service Quality Change

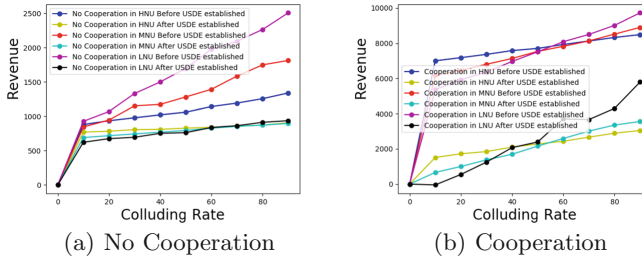
In this section, we will detect the ability of the USDSE to respond to the change of service quality. We tested it in the HCU scenario, a service whose quality oscillates between 1 (low quality) and 5 (high quality). Specifically, the quality of service was 1 in the first 5 cycles and then rose to 5 in another 5 cycles and keep repeating this pattern, we consider two scenarios,

- 1) the service's quality swing from 1 to 5
- 2) the service's quality swing from 5 to 1

From Fig. 6, we can see that USDSE is sensitive to the change of service quality. When the services swing from high quality to poor quality, the obtained results are more accurate. When the quality of the service changes from high to low or low to high, the evaluation of the service of normal users and experts will change, but their reputation will not be changed with the change of service quality. So even if the service Quality changes, our models can quickly monitor changes in service and give a fair assessment of service.



(a) Beginning with low quality (b) Beginning with high quality

Fig. 6. Response to service quality change**Fig. 7.** Revenue analysis of employing malicious users

3.5 Revenue Analysis of Employing Malicious Collusive Users

Figure 7 shows the revenue of employing the collusive users in three scenarios (HNU, MNU, LNU) when no cooperation (Fig. 7(a)) and cooperation (Fig. 7(b)) among service providers (the procedure could be seen in Fig. 3).

With the proportion of collusive users increasing, the revenue is gradually increasing. At the same time, we can see from Fig. 7(a) that in the three scenarios, after the USDSE filter out the malicious user's evaluation, the revenue is almost the same in the end. The reason why the revenue starts to decline at the beginning in Fig. 7(b) is that the correction of evaluation in USDSE and increase of communication cost caused by cooperation. We noticed that the revenue in LNU is higher than in HNU to the end. That's because some collusive users aren't been identified with the increase of the collusive users.

4 Related Work

At present, researchers mainly obtain fair evaluation of users from two aspects: comment and rating of users. Some studies judge the correctness of comment by a single feature of the comment. Wu et al. [26] believe that consumers are more likely to accept recommendations from reviewers when historical ratings in a product area vary widely. [9] present a novel method called DeFrauder to detect and rank fraud reviewer groups. There are studies that use sentiment

analysis to judge false comments. Li J et al. [12] analyze the emotional words in user comments and analyze the semantics of the text from the perspective of emotional polarity, indicating that the false comment contains more emotional words. Franklin et al. [21] propose a method to determine the polarity of comments based on CIAA (confidentiality, integrity, availability, and authentication) related keywords. [20] propose a method called SentiDraw that uses star ratings of reviews to develop domain-specific emotional dictionaries to determine polarity.

Due to the diversity of the comment, it is necessary to determine which factors will affect the quality of the user's comment and speculate on these factors in advance. [3] present a new reputation system using machine learning to predict the reliability of consumers from their profile, which may be a potential solution for future reputation systems.

Many studies use feedback ratings to get fair reviews, so researchers often need to filter malicious feedback ratings. A.Josang et al. [8] assume that the user feedback score follows the beta distribution. They use the sensitivity coefficient q to roughly indicate the percentage of dishonest feedback. The smaller the q value, the lower the false positive rate, and the more false negatives in dishonest feedback. However, the method of A.Josang assumes that user feedback follows a specific distribution, and Weng [25] proposes a new entropy-based method to measure the quality of evidence and further filter unfair evaluations. The proposed method does not require assumptions about the distribution of ratings. Considering the aggregation of malicious user comment time, Yang et al. [28] use statistical methods to detect the time interval of malicious feedback. Considering the complex attack scenarios, the performance of these methods has some limitations. Cai et al. [7] propose a two-phase approach for fraudulent rater detection.

5 Conclusion

The proposed model utilizes the service to evaluate the users, establishes the users' reputation, filters the malicious users, and provides a fair evaluation of users. Experimental results show that our model can effectively identify malicious users compared with HMRep and we can see that USDSE is sensitive to the change of service quality. The USDSE can reduce the revenue of employing collusive users in different scenarios. In essence, USDSE is to improve the objectivity and fairness of users' evaluation from two different dimensions: evaluation of users and evaluation of services.

In the future, we will establish a user-service double-side evaluation model in the ecosystem and verify the validity of the model through real data. At the same time, we will consider the impact of silent users when getting fair evaluation and use more user information to help the service evaluate users.

Acknowledgements. This work is supported by the Foundation of Jiangxi Educational Committee under Grant No. GJJ210338, the National Natural Science Foundation of China (NSFC) under Grant No. 61962026, the National Natural Science Key Foundation of China grant No. 61832014 and No. 62032016, the Natural Science Foundation of Jiangxi Province under Grant No. 20192ACBL21031.

References

1. Akoglu, L., Chandu, R., Faloutsos, C.: Opinion fraud detection in online reviews by network effects. In: ICWSM, vol. 13, pp. 2–11 (2013)
2. Allahbakhsh, M., Ignjatovic, A.: An iterative method for calculating robust rating scores. *IEEE Trans. Parallel Distrib. Syst.* **26**(2), 340–350 (2015)
3. Alqwadri, A., Azzeh, M., Almasalha, F.: *Appl. Mach. Learn. Online Reput. Syst.* **18**(3), 11 (2021)
4. Arora, U., Dutta, H.S., Joshi, B., Chetan, A., Chakraborty, T.: Analyzing and detecting collusive users involved in blackmarket retweeting activities. *ACM Trans. Intell. Syst. Technol.* **11**(3) (2020). <https://doi.org/10.1145/3380537>
5. Baek, H., Jang, M., Kim, S.: Who leaves malicious comments on online news? An empirical study in Korea. *Journal. Stud.* **23**(4), 432–447 (2022). <https://doi.org/10.1080/1461670X.2022.2031258>
6. Byun, H., Jeong, S., kwon Kim, C.: SC-COM: spotting collusive community in opinion spam detection. *Inf. Process. Manag.* **58**(4), 102593 (2021). <https://doi.org/10.1016/j.ipm.2021.102593>, <https://doi.org/10.1080/1461670X.2022.2031258>
7. Cai, Y., Zhu, D.: Who can we trust: A new approach for fraudulent rater detection in reputation systems. *Decis. Sci.* **51**(1) (2020)
8. Commerce, B.E., Jøsang, A., Ismail, R.: The beta reputation system. In: In Proceedings of the 15th Bled Electronic Commerce Conference (2002)
9. Dhawan, S., Gangireddy, S., Kumar, S., Chakraborty, T.: Spotting collective behaviour of online frauds in customer reviews. In: Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence (IJCAI-2019) (2019)
10. Hajek, P., Barushka, A., Munk, M.: Fake consumer review detection using deep neural networks integrating word embeddings and emotion mining. *Neural Comput. Appl.* **32**(1) (2020)
11. Li, B., Song, R., Liao, L., Liu, C.: A user-oriented trust model for web services. In: 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, pp. 224–232. IEEE (2013)
12. Li, J., Ott, M., Cardie, C., Hovy, E.: Towards a general rule for identifying deceptive opinion spam. In: Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics, vol. 1, pp. 1566–1576 (014). <https://doi.org/10.3115/v1/P14-1147>
13. Limam, N., Boutaba, R.: Assessing software service quality and trustworthiness at selection time. *IEEE Trans. Softw. Eng.* **36**(4), 559–574 (2010). <https://doi.org/10.1109/TSE.2010.2>
14. Liu, M., Shang, Y., Yue, Q., Zhou, J.: Detecting fake reviews using multidimensional representations with fine-grained aspects plan. *IEEE Access* **9**, 3765–3773 (2021). <https://doi.org/10.1109/ACCESS.2020.3047947>
15. Maarouf, I., Baroudi, U., Naseer, A.R.: Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. *IET Commun.* **3**(5), 846–858 (2009)

16. Martens, D., Maalej, W.: Towards understanding and detecting fake reviews in app stores. *Empir. Softw. Eng.* **24**(6), 3316–3355 (2019)
17. Nguyen, H.T., Zhao, W., Yang, J.: A trust and reputation model based on Bayesian network for web services. In: 2010 IEEE International Conference on Web Services, pp. 251–258. IEEE (2010)
18. Oh, H.K., Jung, J., Park, S., Kim, S.W.: A robust reputation system using online reviews? *Comput. Sci. Inf. Syst.* **17**, 7–7 (2020)
19. Rezvani, M., Rezvani, M.: A randomized reputation system in the presence of unfair ratings. *ACM Trans. Manage. Inf. Syst.* **11**(1) (2020). <https://doi.org/10.1145/3384472>, <https://doi.org/10.1145/3384472>
20. Sharma, S.S., Dutta, G.: Sentidraw: Using star ratings of reviews to develop domain specific sentiment lexicon for polarity determination. *Inf. Process. Manag.* **58**(1), 102412 (2021)
21. Tchakounté, F., Pagor, A., Kamgang, J.C., Atemkeng, M.: Cjaa-repdroid: a fine-grained and probabilistic reputation scheme for android apps based on sentiment analysis of reviews. *Fut. Internet* **12**(9), 145 (2020)
22. Wang, M., Wang, G., Zhang, Y., Li, Z.: A high-reliability multi-faceted reputation evaluation mechanism for online services. *IEEE Trans. Serv. Comput.* **12**, 836–850 (2016)
23. Wang, N., Yang, J., Kong, X., Gao, Y.: A fake review identification framework considering the suspicion degree of reviews with time burst characteristics. *Exp. Syst. Appl.* **190**, 116207 (2022). <https://doi.org/10.1016/j.eswa.2021.116207><https://www.sciencedirect.com/science/article/pii/S0957417421015219>
24. Wang, S., Zheng, Z., Wu, Z., Lyu, M.R., Yang, F.: Reputation measurement and malicious feedback rating prevention in web service recommendation systems. *IEEE Trans. Serv. Comput.* **8**(5), 755–767 (2015)
25. Weng, J., Miao, C., Goh, A.: An entropy-based approach to protecting rating systems from unfair testimonies. *IEICE Transactions* 89-D, 2502–2511 (09 2006). <https://doi.org/10.1093/ietisy/e89-d.9.2502>
26. Wu, X., Jin, L., Xu, Q.: Expertise makes perfect: How the variance of a reviewer’s historical ratings influences the persuasiveness of online reviews. *J. Retail.* **97**(2), 238–250 (2021). <https://doi.org/10.1016/j.jretai.2020.05.006>, <https://www.sciencedirect.com/science/article/pii/S0022435920300270>
27. Yang, B., Liu, Y., Liang, Y., Tang, M.: Exploiting user experience from online customer reviews for product design. *Int. J. Inf. Manag.* **46**, 173–186 (2019). <https://doi.org/10.1016/j.ijinfomgt.2018.12.006>, <https://www.sciencedirect.com/science/article/pii/S0268401218305437>
28. Yang, Y., Sun, Y., Kay, S., Yang, Q.: Defending online reputation systems against collaborative unfair raters through signal modeling and trust. In: SAC ’09: Proceedings of the 2009 ACM Symposium on Applied Computing, pp. 1308–1315 (2009). <https://doi.org/10.1145/1529282.1529575>