Detection and Adjustment of Malicious User Ratings for Measuring Web Service Reputation

Govinda. K [1] G Aswani Kumar Reddy [2] G Abhishek Varma[3]
[1]Asst. Professor
[1, 2, 3] SCSE, VIT University

Abstract---In services computing domain, Web service reputation is usually calculated using ratings given by service users. However, the existing of malicious ratings and different preferences of different service users often lead to a chance towards positive or negative ratings. In this paper, we propose a novel reputation measure method for Web services. The proposed method detects malicious rating and adjusts rating to enhance the reputation measure accuracy. Here we detect malicious user ratings by cumulative sum method and reduce the negative effect of unfair ratings.

Keywords: Web Service, Cumulative Sum, feedback ratings, Malicious.

I. INTRODUCTION

Web service supports quickly creation of New, applications that can work on different architectures and computing platforms. Web service users can access a large pool of services with varying non- functional qualities providing equivalent or similar functionalities. With the increasing number of Web services in the Internet, it is necessary to select a Web service that provides the best performance from as set of Services.

Normally Web service selection preaches is usually based on the promised qualities by service providers. However, service providers may make quality promises on the published services but fail partially or fully to deliver on these promises at runtime. However, it is not an easy task since some service providers may not perform what they promise. Reputation of the providers needs to be considered when making selection. Hence, accurate reputation measure of Web services is crucial for business applications. The discovered services can be evaluated and ranked according to the feedbacks from service users.

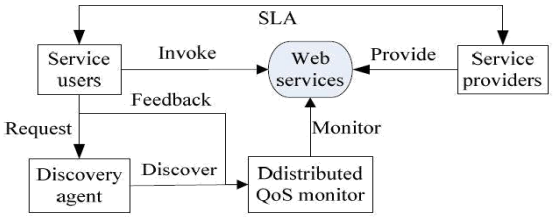

Fig. 1: Web service rating Framework

Several works have been carried out to recognize the importance of reputation measure of Web services. The proposed solutions use different techniques and study different aspects to measure Web service reputation based on user feedback ratings. Although previous work on existing solutions has explored the efficiency and robustness of measure approaches, most of them suffer from the following weaknesses.

It is difficult to ensure the accuracy of feedback ratings. There is a large variety of service users on the Internet. Service users can express their preferences over Quality of Service (QoS) attributes of services. The user ratings are often subject to service users' preferences. As some service users are conservative (tend to provide low ratings on various Web services), whereas some others may be aggressive or neutral. Hence, different service users often give different ratings to the same used service.

In this paper to eliminate these drawbacks and improve the accuracy of reputation measure of Web services we propose a new method called Cumulative Sum and reciprocal Coefficient to co-relate user ratings and to find malicious ratings and to lessen the influence of malicious ratings on the trusted reputation measure.

This paper is organized as follows Section II describes related work carried out. Section III describes proposed reputation measure method, which contains malicious rating detection and adjustment. Section IV analysis on our method compared to other methods. Section V concludes the paper.

II. MALICIOUS RATING DETECTION AND ADJUSTMENT METHOD

The reputation of a Web service Depends on collective feedback rating of the users that have interacted with or used it in the past. Feedback rating is the perception of each user about services it has invoked. It could be a single value representing an overall perception or a multi value for each QoS parameter of Web service, such as response time, reliability and availability.

A. Previous Method:

In this study, for each service *si* that it has invoked, a service user provides a feedback rating indicating the level of Satisfaction with a service after each Interaction with the service. A rating is simply an integer ranging from 1 to 10, where 10 means extreme satisfaction and 1 means extreme dissatisfaction. Then service users maintain *n* feedback ratings representing their perception of *si*'s performance. We take *q* (*si*) to represent the reputation score of *si* in a global time. Then q (*si*) can be calculated by using

$$q(s_i) = \frac{1}{n}\sum_{i=1}^{n} r_i$$

Where *ri* represents the *i*-th feedback rating. The above rating mechanism has severe drawback so we employ our new reputation method by eliminating Malicious rating.

B. Proposed Method

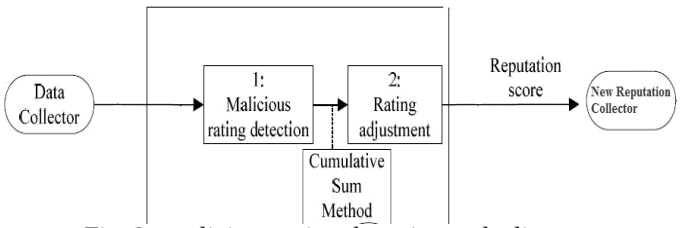

Fig. 2: malicious rating detection and adjustment

As shown in Figure 2, our method mainly contains two phases i.e., Malicious rating detection and rating Adjustment. The first phase involves detecting malicious feedback ratings collected by Data Collector using Cumulative Sum Method. The second phase involves computing feedback similarity of different service users to Adjust ratings. Finally, new reputation scores measured are stored and provide the scores when requested by Discovery agent

1) Phase-I: Malicious rating detection

Malicious ratings must be considered in reputation measure of Web services. In this phase, we apply Cumulative Sum Method (CUSUM) to detect and handle malicious ratings. The CUSUM belongs to the family of change point detection algorithms that are based on hypothesis testing, and was developed for independent and identically distributed random variables *{yi}*. According to the algorithm, there are two hypothesis $\theta 0$ and $\theta 1$, with probabilities $p\theta 0$ and $p\theta 1$, where the first corresponds to the statistical distribution prior to a change and the second to the distribution after a Change.

$$C_n = \sum_{i=1}^{n} c_i$$

Where $c_i = \ln \frac{p\theta_1(y_i)}{p\theta_0(y_i)}$.

The typical behaviour of the log ratio includes a negative drift before a change and a positive drift after the change. CUSUM is well suited for checking a measuring system in operation for any departure from some target or specified values and have been widely used for detecting the small and moderate mean shifts.

Malicious feedback ratings can be of two types

a) Positive malicious feedback ratings:

A service provider indulges with a group of service users in order to give unfairly high ratings by them. For instance, a malicious user reports a rating that is 10 for a poor service.

b) Negative malicious feedback ratings:

Service providers can indulge with service users in order to "Bad-mouth" other service providers that they want to drive out of the market.

In such a situation, the conspiring service users provide unfairly negative ratings to the targeted service, thus lowering their Reputation.

For each feedback rating CUSUM monitors a set of *n* rating sample intervals *{y*1, · · ·, *yn}*. *yn* is the sum of all ratings in the *n*-th sample interval. Assume the change rating traffic *{yi}* is independent Gaussian distribution with known variance $\sigma 2$,which we assume remains the same after the change, and $\mu 0$ and $\mu 1$ are the mean rating traffic before and after the change. Then CUSUM can be described as follows:

$$f_n = \left[f_{n-1} + \frac{\mu_1 - \mu_0}{\sigma^2} (y_n - \frac{\mu_1 + \mu_0}{2}) \right]$$

Where $fn = Cn - mn$ and $mn = \min Ci$

2) Phase-II: Malicious rating adjustment

In addition, to adjust ratings we apply CUSUM to *xn*, with $xn = xn - \mu n-1$, where *xn* is the sum of all feedback ratings in the *n*-th sample interval, and $\bar{\mu} n$ is an estimate of the mean rate at the *n*-th sample interval.

$$f_n = \left[f_{n-1} + \frac{\mu_1 - \mu_0}{\sigma^2} (x_n - \bar{\mu}_{n-1} - \frac{\mu_1 + \mu_0}{2}) \right]$$

By the above formula we can adjust the ratings for given interval to get correct web- service rating for effective measurement.

III. RESULTS

Here we have taken some malicious user ratings of a web service and given a plot of Users Vs Ratings

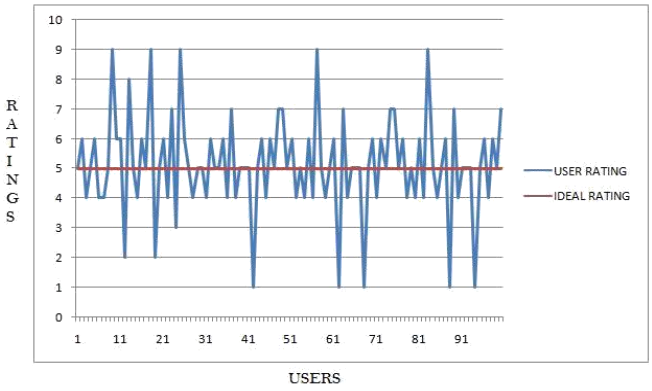

Fig. 3: User malicious ratings

We have detected the malicious ratings by using our approach and adjusted reputation of web service

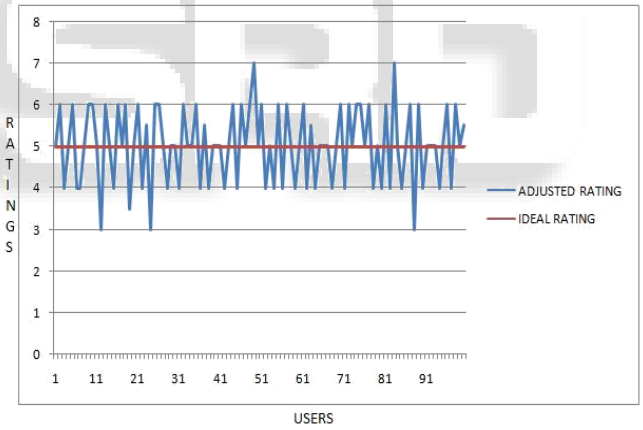

Fig. 4: Adjusted ratings

IV. RELATED WORK

D. Ardagna and B. Pernici [3] proposed a service composition approach where reputation is one of five QoS attributes considered. Although the approach is effective to find the best composition service, it considers little the truth and objectiveness of feedback ratings from users.

W. Conner et al. [4] Proposed a reputation-based trust management framework that supports the synthesis of trust-related feed- back from multiple services hosted within an infrastructure. The core of the framework is trust management service (TMS).

TMS allows each service to use its own trust metrics to meet its local trust requirements and supports multiple reputation scoring functions. The framework has a significant advantage that supports multiple reputation measure approaches, which

are suitable to multiple web service environments. TMS takes the client, the service, the normalized transaction feedback value and the set of optional attributes to create a service invocation history record.

The record is used to measure the r e p u t a t i o n, which is more accurate and reasonable than the calculation method in [3]. S. Nepal et al. [5]

Z. Yanzhen et al. [10] proposed an approach for rectifying the prejudicial feedbacks ratings to increase the accuracy and the reliability of reputation based trust evaluation in the situation that feedback data are lacking or are insufficient based on their proposed trust model.

The proposed trust model can minimize the extent to which a malicious service provider behavior maliciously while retaining high trust value. At the same time, it can discourage these services with low QoS to attain high trust value by behaving non- maliciously over a period of time. The key of the approach is to reduce the effects of the prejudicial feedbacks by adding or decreasing its corresponding offset.

V. CONCLUSION

In this paper, we point out the limitations of the existing rating adjustment measure approaches and propose a malicious rating detection and adjustment measure method to develop reliable reputation systems for Web services based on feedback ratings.

In the future, we plan to conduct real-world usage studies to further verify our proposed method. Moreover, we will investigate how to adjust the method to provide better performance to real world service users

REFERENCES

[1] S. Wang, Q. Sun, and F. Yang. Towards web service selection based on QoS estimation. International Journal of Web and Grid Services, 6(4): 424-443, 2010.
[2] Z. Malik and A. Bouguettaya. Evaluating rater credibility for reputation assessment of web services. In Proceedings of the 8th International Conference on Web Information Systems Engineering (WISE'07), pages 38-49, 2007.
[3] D. Ardagna and B. Pernici. Adaptive service composition in flexible processes. IEEE Transactions on Software Engineering, 33(6): 369-384, 2007.Nahrstedt. A trust management framework for service-oriented environments. In Proceedings of the 18th international conference on World Wide Web (WWW'09), pages 891-900, 2009.
[5] S. Nepal, Z. Malik, and A. Bouguettaya. Reputation Propagation in Composite Services. In Proceedings of the IEEE International Conference on Web Services (ICWS'09), pages295-302, 2009.
[6] R. Jurca, B. Faltings, and W. Binder. Reliable QoS monitoring based on client feedback. In Proceedings of the 16th international conference on World Wide Web (WWW'07), pages 1003-1012, 2007.
[7] N. Limam and R. Boutaba. Assessing Software Service Quality and Trustworthiness at Selection Time. IEEE Transactions on Software Engineering, 36(4): 559-574, 2010.
[8] J. R. Douceur. The Sybil Attack. In Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS'01), pages 251-260, 2002.
[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman. Sybil- Guard: Defending against Sybil attacks via social networks. IEEE/ACM Transactions on Networking, 16(3): 576-589, 2008.
[10] Z. Yanzhen, G. Liang, L. Gee, X. Bing, and M. Hong. Rectifying prejudicial feedback ratings in reputation based trust management. In Proceedings of the IEEE International Conference on Services Computing (SCC'07), pages 530-535, 2007.
[11] F. Li, F. Yang, K. Shang, and S.Su. A Policy-Driven Distributed Framework for Monitoring Quality of Web Services. In Proceedings of the IEEE International Conference on Web Services (ICWS'08), pages 708-715, 2008.
[12] S. Ries and E. Aitenbichler. Limiting Sybil Attacks on Bayesian Trust Models in Open SOA Environments. In Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC'09), pages 178- 183, 2009.
[13] V. A. Sires and F. Papagalou. Application of anomaly detection algorithms for detecting SYN flooding attacks. Computer Communications, 29(9): 1433-1442, 2006.
[14] R. Radharamanan, A. Galelli, D. T. Alex, and L. L. Perez. Sensitivity analysis on the CUSUM method. International Journal of Production Economics, 33(1): 89-95, 1994.
[15] C. Delarosa's. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior.

