A Survey Study on Reputation-based Trust Mechanisms in Service-Oriented Computing

Suronapee Phoomvuthisarn

Mahanakorn University of Technology, Thailand
E-mail: suronape@mut.ac.th

ABSTRACT – The Reputation-Based Trust mechanism (RBT) helps a service assess the trustworthiness of offered services, based on the feedback obtained from their users. A key challenge to apply the RBT is to prevent the cheating behavior of users when they provide recommendations -- they might give unfair ratings to benefit themselves. This survey describes the research communities that are making efforts to solve the problems of the RBT in Service-Oriented Computing (SOC) domain. A summary of findings is then discussed to position the trends and directions of future studies. The survey can be used as a reference guide in a hope to make trust-based service systems more reliable and scalable.

KEYWORDS – Trust Systems, Software Architecture, Service-Oriented Computing

1. Introduction

The Reputation-Based Trust mechanism (RBT) [2] has become an increasingly active research area in SOC since its successful application in many areas, such as e-commerce, multi-agents systems, and P2P systems [22]. The RBT provides an effective means of assisting services to minimize risk in their future interactions, especially when they have no prior historical records about others [46]. Yet, owing to the accumulation of unfair ratings, the RBT still has a problem regarding the quality of reputation information. As reported by many studies, such as [18] for fake positive reviews in Amazon, and [30] for numerous negative comments for hotels in TripAdvisor.com, some service users intentionally lie in their feedback in order to gain benefits from the biased reputation that they themselves establish. Based on this large amount of evidence that such feedback can be manipulated, the reputation produced by the RBT cannot be used with full confidence to identify a service's trustworthiness [22] [68] [57]. An increasing number of publications, such as [35] [33] [37] [42], address this weakness by trying to develop mechanisms to help the RBT ensure a robust reputation. A few studies, such as [59] [62] [70], have investigated the overhead costs incurred by these proposed mechanisms when they are integrated with the original trust systems.

Judging by a research gap in the current literature [26] [29] [65] [16] [37] [42], the mechanisms currently proposed fail to discourage raters (i.e., service users that rationally provide ratings to other services) from rating other services untruthfully, especially when the unfair raters are in the majority. In addition, little attention has been paid to the issues of integrating the proposed mechanisms with the trust systems. The limitations of these mechanisms thus establish a context for further investigation in this survey.

This survey presents a comparison of various proposed mechanisms currently in use to help the RBT prevent cheating by raters. A summary of findings is then discussed to position the trends and directions of future studies in a hope to make trust-based service systems more reliable and scalable.

The structure of the survey is as follows: First, Section 2 discusses the background of the RBT and its main problems in the context of SOC. Section 3 then presents an overview of existing research that attempts to solve the problems of the RBT. Next, a summary of findings is discussed in Section 4 to

position these studies for this survey. Section 5 proposes the research directions posed by the RBT problems. The survey ends with a summary in Section 6.

2. Background

2.1 The Reputation-Based Trust mechanism (RBT)

Reputation-based trust mechanism is a mechanism using feedbacks reported by other parties to identify good from bad target parties [2]. The main role of the RBT is to gather feedbacks from parties, to aggregate all of these feedbacks into a meaningful information (e.g. reputation scores), and to disseminate this information as publicly known by others.

Existing RBTs differs in several dimensions. The first is the format of feedback elicited. Some mechanisms requires the format of feedback in terms of a binary (e.g., positive and negative in eBay (2010), a finite number of positive values (e.g., five stars for books in Amazon (2010), or even textual comments in eBay (2010). The second dimension is the way they aggregate feedbacks into reputation information. Some mechanisms simply sum up the number of positive ratings and negative ratings separately in eBay (2010) into reputation scores or even compute these feedbacks as the average of all ratings. A slightly advance models computes a weight average of all the ratings where the ratings can be determined by factors such as the trustworthiness of the party providing ratings. Finally, the third dimension relates to how the resulting reputation is disseminated in the community. Some mechanism relies on the centralized party to accumulate all feedbacks, compute them into reputation information and, keep this resulting information in centralized nature. Once enquired about one party's reputation, the centralized party then queries one specific reputation information stored to the enquiring party. Other mechanisms rely on decentralized infrastructure where each participating party is responsible for storing and computing their partners' reputation themselves. The reputation information is enquired on demand through social networks.

To simplify the understanding of the RBT in SOC, this survey utilizes the common RBT [22] used by many researchers as follows:

$$Reputation = \sum_{i=1}^{n} w_i \times rating_i \qquad (1)$$

where wi represents a weighted reputation ε 0..1 of a rater, ratingi represents a rating rated by a rater i, and n represents a number of raters.

From the above equation, the reputation score is a measure of a provider's trustworthiness in SOC. It can be computed by collecting ratings from other services that have previously interacted with the provider. The reputation of one provider can be calculated by aggregating its ratings submitted by raters into one percentage measure Reputation ε [0..1], each of which is weighted by raters' reputation [22] as shown in Eq.1.

2.2 The RBT and its Challenges for a QoS-based Service Selection Process

In the area of SOC, there have been a number of approaches to using the RBT in trust management, especially for service selection. Keys among these works include [56] [38] [60] [3] [29]. The common aim of these approaches is to distinguish good behavioral services from bad ones [22]. After the functional aspects, Quality of Service (QoS) is the next most important factor in making selective decisions in SOC [55] [58]. QoS helps services to know how well one service can do in terms of non-functional properties (e.g., response time and availability) and differentiates the best service from a number of services offering similar functionalities.

The basic idea behind this work is to utilize a centralized QoS registry, such as UDDI [43], for accommodating QoS information published by a providing service (a provider), and to evaluate the provider's reputation (i.e., the reputation derived from providing the QoS information) based on the reputation scores computed from ratings collected from raters [58] [68]. According to the QoS information and the reputation scores computed, the QoS registry then ranks providing services based on requesting services' preferences in the service discovery request. These reputation scores will be returned to the requesting services to help them decide whether to interact with the providers. A providing service with a higher reputation has a high probability of honestly providing the service it offers with the QoS information as claimed.

There are two main problems for the trust systems in the use of the RBT in SOC.

The first problem is that of unfair ratings. This problem occurs when raters conspire to provide ratings or recommendations that are misleading and redound to their own benefit [56] [22] [25] [68] [59]. For example, a providing service might collude with some raters to rate its offered services as positive in order to enhance its reputation. Alternatively, a providing service might be targeted by some raters aiming to damage its reputation by giving it negative ratings. As reported by many studies, there is a large amount of evidence that such ratings can be manipulated. One research study [47] found that more than 98% of all ratings provided by raters are negative, since the raters expect to boost their own position relative to their rivals or alternatively to avoid negative ratings for retaliation. The bias of ratings mainly due to reciprocal effects is also mentioned by [7] and [31]. Harmon [18] reports that some Amazon users fake positive reviews to boost the sale of their own books. Elliott [15] reveals in their studies that some hotels on TripAdvisor.com deliberately lower their competitors' reputation by negative ratings. Therefore, the reputation gathered from ratings such as these is compromised and cannot be used with full confidence to determine the trustworthiness of individual services (e.g., service provider). Complementary to these studies, the trust systems leveraging the RBT in SOC also need a potential mechanism to be integrated to prevent cheating behavior by raters.

Second, while cheating behavior is a major research topic relating to the RBT, most of the existing research, including [33] [36] [66] [37] [16] [42], focuses solely on state-of-the-art theories and applications of statistical processes to devise mechanisms additional to the RBT to address the problem. This trend and direction of research design leaves a gap in the literature. These studies can only prove their devised mechanisms on a small scale, mostly in a centralized nature, thus leaving open the question of the extent to which their mechanisms can function without degrading the existing trust systems as well as their extension to support large-scale service systems in fully distributed environments such as SOC.

3. Existing Studies and Their Limitations of the RBT

Two problems constitute the related work for this research: the problem of unfair ratings due to cheating behavior of raters, and the lack of suitable distributed architectures to support integrated mechanisms, designed to enhance trust systems with a capability to prevent lies. This section provides insights from an analysis of existing research work that attempts to solve problems in both of these areas.

3.1 Problem 1 – Unfair Ratings

3.1.1 Detective Methods - Many proposals in SOC have employed statistical techniques from previous research work in e-commerce, P2P, and multi-agent systems to tackle the problem of cheating behavior for a QoS-based service selection. Such techniques, including iterated filtering approach [61], clustering and correlation techniques [14] [48] [36] [66] [67] and the similarity distance between two different groups EigenTrust [1] XRep [11] [27] [64] [33], treat unfair ratings as outliers of the samples. These small samples can be detected and excluded as unfair ratings based on statistical data; the systems automatically 'learn' to recognize complex patterns and make intelligent decisions to help the trust systems foresee the trend of untruthful behavior. In the same spirit, many works in SOC have applied these statistical techniques to detect unfair ratings given by raters to one particular service. Keys among these works include [35] [56] [29] [37] [42].

Although these detective techniques provide a promising approach to predict the trend of unfair ratings for evaluating the reputation of a service, they face two main drawbacks. First, detective techniques cannot produce accurate estimates of a service's reputation when the majority of raters lie. This is because statistical techniques such as collaborative filtering assume that most raters provide fair ratings and filter the false rating based on their similarity with the majority [14] [61]. Therefore, if the majority of ratings are unfair, the reputation gathered from these majority samples could misrepresent one service's trustworthiness. Therefore, this method cannot produce reputation information correctly when dishonest raters are the majority in the community.

Second, these techniques lack sufficient ratings to foresee correctly the trend of untruthful behavior. The main reason for this is that they do not provide clear incentive schemes to motivate raters for providing ratings to others [45] [41] [8]. As reported by many studies, raters are reluctant to put an effort into providing ratings to others unless they gain some benefit in return. One study [19] conducted a survey and noted that economic incentives such as rewards gained after submitting a review are one of the core factors in motivating raters to submit online feedback. Another study [20] conducted an experiment with users on providing feedback for books on Amazon; it found that users who have a moderate outlook are not likely to report unless they are provided with some benefit. A third study [53] also pointed out that

some incentives must be given to raters in order to motivate them to voice their opinions. Based on these findings, it can be said that using detective techniques without clear incentive schemes will result in a biased reputation being quantified from unrepresentative samples collected. As a result, the trends of untruthful behavior cannot be used correctly to detect unfair ratings, and may even misrepresent a service's reputation due to insufficient ratings being captured.

To overcome this shortcoming, several proposals suggest augmenting specialized monitoring agents to monitor all ratings reported. Their aim is to solve the problem of unfair ratings accumulated by detecting all of the actual ratings provided. In this way, robust ratings can be captured – ratings on response time or availability, for example – thus producing accurate estimates of the reputation score for requesting services. Keys among these research works are the following: [9] [13] [38] [54] and [51]. However, these approaches are not suitable for large-scale service systems in SOC, since the monitoring agents would need to collect the information intensively from execution monitoring of all available raters. This solution would therefore be expensive in reality [56] [58].

3.1.2 Preventive Methods - The limitations of detective methods have stimulated intensive research into developing incentive techniques (or so-called "preventive mechanisms" [69]) to eliminate or to obviate incentives to lie. Unlike detective approaches [37] [42] aiming to detect unfair ratings, preventive mechanisms give raters some incentive (e.g., digital currency or credit) so that truthful reporting maximizes the raters' expected revenue, thus discouraging them from deviations in reporting the truth [25].

Market-based approaches in economics play a major role in the design of these mechanisms. Such approaches – in particular, game theory [52] – have emerged as methods that put a powerful advantage to work in an applied environment [49] [31]. Their advantage lies in their ability to predict, based on the information available to them, agents' actions that correspond to that information. They assume that agents are fully rational in their reasoning about all information and that the agents will tend to choose the option that will yield them the highest payoff (i.e., the benefit obtained, such as money) [17] [44]. The advantage of market-based approaches is that they can provide plausible solutions in many computer science research projects [31] such as trust [32], that are influenced by human subjects with different incentives.

In trust-based domains, the concepts of game theory [52] have been adopted in SOC to help elicit private information from services, such as raters. The preventive mechanisms stemming from this theory are devised and embedded into a reputation model to stimulate raters not only to provide ratings, but also to offer ratings truthfully. There are two categories of preventive methods: (1) the side payment scheme, which encourages rational raters by giving them some kind of monetary incentive, and (2) the reporting game, which rewards participating raters that provide truthful ratings with reputation scores that enhance their creditability. However, no preventive mechanism can claim complete victory in the field. All of them still have the limitations of their own.

(1) Side Payment - Preventive mechanisms based on a side payment scheme [14] [39] offer an appropriate payment to raters that fairly rate others. By providing a payment that offsets any possible incentive to be untruthful, these mechanisms aim to guarantee that lying is not in the rater's best interest.

The study from Jurca and Faltings [23] [25] [26] describes incentive-compatible payment schemes for an agent faithfully to report feedback of other agents. In this approach, a set of distributed broker agents are organized to buy and sell the feedbacks to and from any agents. Ordinary agents can first buy a feedback of any agent from one of the broker agents, and once they have finished the transaction with that agent, the ordinary agent can sell that agent's feedback back to one of the broker agents. The author makes faithful reporting an optimal strategy by devising a payment scheme that pays a submitted feedback if it has the same value as randomly chosen feedbacks from other agents. In a similar way, Miller et al. [40] provide an incentive for buyers to be truthful that is based on proper scoring rules [21] [28] [10]. This approach uses a central processing store to reward buyers with an appropriate payment based on the correlation of their reports with those of other buyers. Recent studies that apply proper scoring rules include [70] [62]. In the same spirit, Gerding [16] proposes an incentive mechanism to elicit and fuse costly estimates from nominated multiple suppliers. This model pays a side payment to those suppliers who submit the same ratings as the majority. Another study [65] proposes a file evaluation method for a user. The method requires the rater to download its file; the user can evaluate the downloader in order to give a proper bandwidth quota as well as a position in a waiting queue. Their model implements a payment scheme for raters to get some payment if their vote is the same as the majority of votes from others.

There are two problems with preventive mechanisms based on the side payment scheme. First, these approaches commonly have difficulty ensuring truthfulness when the majority of the raters lie about their ratings. This is because these approaches rely on statistical techniques that treat the majority of samples as fair ratings (just as detective techniques do). These statistical techniques are only effective when the proportion of dishonest raters is almost one half (25% in the study of Dellarocas [14], 40% in the study of Sen and Sajja [48], and 30% in the study of Whitby et al. [61]). Preventive mechanisms using such measures thus cannot ensure truthful reporting of raters when the majority of ratings are unfair. For example, the preventive mechanism from Jurca and Faltings [25] assumes that a rater providing a truthful rating will be rewarded and get paid only if its rating is the same as the next rating of the same rated service provided by another rater. Dishonest raters could gain benefits in terms of the payment being paid to similar ratings as many others, which is unfair. Thus, embedding these preventive mechanisms into trust systems would lead to ineffective solutions to prevent raters from cheating in the majority.

The second problem is that these approaches rely on the common assumption that different raters will have the same opinion of a particular product or service. However, this assumption is not always correct, especially in SOC. The offered service may have inconsistent quality over time [63]. Distinct factors, such as location or satisfaction, can lead raters to perceive the quality of an offered service differently. These mechanisms might wrongly punish some raters who submit truthful ratings, only because they are in the minority. Hence, approaches that assume the majority of samples are fair are not a practical means of ensuring truthful reporting by raters.

(2) Reporting Game - Another type of preventive mechanisms is based on the concept of the reporting game, from game theory [52]. Instead of giving monetary payment to raters who provide truthful ratings, the reporting game measures the reputation value of raters according to their past ratings. This mechanism [24] involves two participants in a game. After each transaction, both participants have an opportunity to rate each other. If the two ratings are different, which indicates that at least one of them is lying, the creditability of both participants is decreased as a punishment. Eventually, both participants will provide truthful ratings to keep up their creditability.

However, these approaches are still based on comparison of feedbacks. The schemes compare the feedbacks with the other participant's feedbacks in a previous transaction. Therefore, this comparison-based approach cannot ensure truthful reporting of raters when untruthful raters are in a majority; unfair raters could gain benefits based on unfair ratings given to others if the other rater is dishonest.

Another study that casts doubt on a comparison-based approach in the reporting game is the work from [70]. The authors model the process of truthful reporting as a repeating game to encourage raters to truthfully provide feedback to others. Their approach derives a minimum local wage payment using numerical solutions to reinforce the truthful strategies of raters. This payment is computed for the requesting service to offer the rater to truthfully declare the reputation of a providing service, whether it fails or succeeds in conducting the transactions with the rater. Although this approach does not require requesting services to verify and compare the information truthfulness of raters with their ratings, its wage-based incentive mechanism still cannot ensure truthful reporting when the majority of raters lie. This is because the scheme still relies on probability distribution of the previous successful and failed transactions in order to devise appropriate utility to raters in the rewarding and punishment process. In addition, the scheme also assumes that requesting services are more interested in failed transactions than in successful transactions. Therefore, the utility gains of raters are not derived appropriately to ensure truthful reporting based on the unbalanced nature of feedbacks.

3.2 The Lack of Suitable Distributed Architectures for Extra Mechanisms

Since cheating behavior is a major research topic relating to the RBT, most previous study, including [39] [23] [35] [56] [65] [16] [37] and [42], has focused on devising a mechanism to solve the problems of raters' cheating behavior. Only a few studies [59] [62] [70] have investigated the overhead costs incurred by these proposed mechanisms when they are integrated with the original trust systems. Yet, in the absence of a proper integration technique, the integrated mechanism might increase the overhead costs of trust management, especially in terms of interfacing metrics: extensibility, scalability, decentralization and performance quality attributes, making the trust systems inefficient or even causing them to fail.

The need for suitable distributed architectures to support the extra mechanisms is underlined by two principal findings in previous research. First, most of the mechanisms proposed to prevent lying are

heavily computation intensive. These approaches [23] [65] [16] mostly require detecting all actual ratings submitted by raters and require a correspondingly long computation time to produce complete and accurate estimates of all the raters' payments. Thus, the computational overhead caused by integrating such mechanisms might outweigh the gain obtained from preventing unfair ratings [5]. This poses a number of risks in terms of integrating the proposed mechanisms with the original trust systems while achieving extensibility and performance quality attributes.

There is some body of work that tries to diminish this concern; however, these studies do not completely address the issue of an extra overhead during the integration process. One study [62] evaluates the efficiency of its proposed mechanism in terms of the consumption of computing resources (i.e., CPU usage). However, the test for integrating its mechanism with trust systems is missing, so it does not establish whether mechanisms can scale without degrading the original trust systems. Wang et al. [59] also deal with the overhead cost of integrated mechanisms within trust systems. The authors attempt to investigate the cost and efficiency of the trust systems where such mechanisms are applied. By generalizing individual small groups of networks, the authors can quantitatively analyze the behavior of complex networks based on the mathematical equations. However, their derived equations only take into account the number of raters in the network; they do not consider the integration of the preventive mechanisms proposed. Moreover, they do not conduct an empirical study. Another study is from Zhou et al. [70]. The authors describe the way to integrate their proposed mechanism in the trust systems. This approach integrates the mechanism as a number of exchange messages between participants, realized in relevant layers in a message feedback protocol. But although the authors propose a clear scheme for integrating the proposed mechanisms, the additional costs incurred by these mechanisms are not evaluated empirically. Hence, it is still not clear how far trust systems can function correctly when integrating with the proposed mechanisms.

Second, most of the existing research work, such as [16] [39] [65] and [70], has not focused on exploring how the proposed mechanisms can be composed in distributed systems. Hence, it is unclear how to utilize their mechanisms in SOC, where a central authority does not always exist. These approaches assume the existence of either an infrastructure or a trusted centralized party that maintains the digital currency or reputation scores of participants for the purpose of enforcing their mechanisms' truth-telling properties through rewarding or charging. Therefore, the computation of such approaches is all centralized in the trust system [41]. This imposes research questions concerning their extension to support distributed environments such as SOC, while achieving decentralization and scalability quality attributes.
All of the above demonstrates the need for a proper interfacing technique to facilitate the integration of a potential mechanism with existing trust systems. This facilitation aims at optimizing the overhead costs in terms of interfacing metrics incurred by the integrated mechanism, coupled with a devising mechanism for preventing lies.

4. Summary of Findings

To compare the different approaches, their capabilities may be analyzed on the basis of the four requirements summarized above in Table 1: (1) Maturity, (2) Majority, (3) Cost, and (4) Infrastructure.

In the table, the word "Yes" indicates that an approach has the capability, while "≈ Yes" indicates that an approach has the feature, but in a limited capability. For example, the proposed mechanism from Zhou et al. [70] is capable of ensuring raters' truthful incentives and describes how to integrate their proposed mechanism in the trust systems, but does not empirically evaluate how the proposed mechanism can scale in trust-based domains. The following list gives the four capabilities that a potential mechanism should possess.

Maturity: A potential mechanism should have a clear incentive scheme to motivate raters in providing ratings to others. The mechanism should ensure that raters will not benefit from cheating in any situation. To achieve this, the utility gain needs to be properly derived to reward raters who submit fair ratings and to punish unfair raters who provide untruthful ratings, whether the untruthful ratings are positive or negative.

In addition, the utility gains of the proposed mechanisms should not be transferable, or the proposed mechanisms' properties might not work in a real-world scenario. The preventive mechanisms stem from a sub-branch of game theory called the "non-cooperative game" [4]. The characteristics of this game rely on the strong assumption that players of the game cannot enforce contracts through third parties. Based on this restriction, players cannot commit to anything or make any transfer unless it is part of the game definition itself. Failure to comply with this

condition may result in the violation of the mechanism property.

Since the monetary gain of the side payment scheme can be transferable [25], unfair raters might feel satisfied with the external source of money rather than bidding its true valuation. This generally happens when a rater receives money greater than the cost of reporting the truth. The fact that money is transferable makes preventive mechanisms in the category of a side payment not applicable to some extent. In contrast, the research work based on a reporting game uses reputation as a measure of gain to reward or charge raters. The reputation can be considered as a public opinion of one target party's character or standing; hence, it is considered objective and not transferable, since it represents a collective evaluation of one entity from the point of view of a group opinion [22] [68] [42].

Majority: To ensure truthful reporting even when dishonest raters are in the majority, a potential mechanism should not rely on a measure of gain that depends on the majority of ratings submitted. Most existing studies have difficulty ensuring truthful reporting from raters that are mainly untruthful. Jurca and Faltings [25] try to address this concern by giving a higher reward to the feedback that is similar to many of the reports available for the same service. In their approach, the authors make it possible to ensure truthful reporting of raters in the majority (up to 80%) by giving a higher reward to raters whose feedback is align with many of reference feedbacks. However, since their approach still relies on the assumption that raters will share the same opinion regarding the quality of the service, the use of their mechanism is not practical in reality, especially in SOC. In addition, a means of implementing a reward scheme with monetary incentives makes it difficult to apply this approach in trust-based domains; money can be transferable and does not necessarily correspond to raters' actual interest [12].

Cost: An effective approach should address the costs of integrating a potential mechanism in terms of extensibility and performance quality attributes. It should be empirically tested for to see how far the trust systems with integrated mechanisms can function in their environments. A potential mechanism should also be sufficiently lightweight to capturing enough objective-value representative samples to produce a reputation score correctly with affordable overhead costs. A limited number of studies [59] [70] address the costs, but they do not test their approaches empirically. Hence, it remains unclear to what extent trust systems can function with affordable overhead costs incurred by integrated mechanisms.

Infrastructure: With regard to the characteristics of SOC, an effective approach should design a potential mechanism to support distributed infrastructure. Most traditional approaches are designed based on a central authority that collects ratings from raters in order to derive an appropriate payment for them. However, in fully distributed environments such as SOC, there is no central location for obtaining ratings or performing payment calculations. Thus, applying mechanisms that are designed on a centralized basis is difficult in this environment. Even though some approaches, for example the study by Jurca and Faltings [23] [25] [26], have distributed central services for collecting ratings, it is still partly centralized and therefore not scalable to obtain all ratings from raters.

Based on the investigation of current literature, which is summarized in Table 1, existing mechanisms are currently not up to overcoming the limitations of the RBT: (1) the problem of unfair ratings due to cheating by raters, and (2) the lack of suitable distributed architectures to support integrated mechanisms to prevent lying. Some or all of the four requirements mentioned above are lacking from each of the two preventive methods, which means that neither of them can ensure truthful reporting from raters.

This research gap opens up the possibility for this survey to point out a suitable well-proven preventive mechanism in which the computation does not depend on the majority of samples to integrate with the trust systems to discourage cheating on the part of raters.

Moreover, in discussions of the potential integrated preventive mechanism, little attention has been paid to devising suitable distributed architectures to support the proposed mechanisms. The costs of integrating the proposed mechanisms with the trust systems, as well as the lack of a distributed structure, make it difficult to ensure that these trust systems with the proposed mechanisms integrated can function correctly with affordable overhead costs in SOC.

Proper integration techniques should be applied to ensure that the integration process can still successfully discourage raters from their untruthful incentives without degrading the existing trust systems' capabilities in terms of interfacing metrics: extensibility, scalability, decentralization and performance quality attributes.

Methods	The Mechanisms' Capabilities		Architecture Support	
	Maturity	*Majority*	*Cost*	*Infrastructure*
-Side Payment				
(Miller et al., 2005) [40] (Yang et al., 2007) [65] (Zohar and Rosenschein, 2008) [70] (Gerding et al., 2009) [16]	≈ Yes	-	-	-
(Jurca and Faltings , 2003) [23] (Jurca and Faltings , 2007) [25] (Jurca and Faltings , 2009) [26]	≈ Yes	≈ Yes	-	≈ Yes
(Witkowski, 2009) [62]	≈ Yes	-	≈ Yes	-
-Reporting Game				
(Jurca and Faltings, 2004) [24]	Yes	-	-	-
(Zhou et al., 2011) [70]	Yes	-	≈ Yes	-

Table 1. Efforts Addressing the Problems of the RBT

5. Research Directions

As previously discussed, a well-proven preventive mechanism should be adopted to support the prevention of cheating behavior in such a way that calculating the appropriate payment to promote truthful incentives does not rely on majority samples. In addition, a proper integration technique should be devised to ensure the integration process of such a mechanism with trust systems is efficient, based on the four interfacing metrics: (1) extensibility, (2) scalability, (3) decentralization, and (4) performance quality attributes.

The solutions for answering these research directions are as follows:

(1) A well-proven preventive mechanism to support the prevention of cheating behavior, especially when the majority raters are dishonest.

Apart from its clear incentive schemes and clear empirical proof, the proposed mechanism should potentially be exploited to encourage participants to reveal their private information truthfully when the majority of bids are unfair. Its computation method should not rely on the majority of samples, making it possible to ensure truthful reporting of raters when the majority of them lie. It should also be lightweight in nature in integrating the mechanism into a trust negotiation protocol. The aim is to prevent the trust systems from being exploited by unfair raters while ensuring that the integrated mechanism incurs only affordable overhead costs.

(2) A proper integration technique to ensure the integration process of the proposed mechanism with trust systems is efficient, based on the four interfacing metrics: (1) extensibility, (2) scalability, (3) decentralization, and (4) performance quality attributes.

To facilitate the integration of the proposed mechanism within original trust systems, the concepts of a loosely coupled component-based approach [50] from software architecture can potentially be reused to decompose the overall trust system into functional components. The benefits of such an approach are to support extensibility and maintainability in highly dynamic environments. Hence, without degrading the existing trust-based capabilities, the architecture-based approach should be utilized to facilitate the integration of the proposed mechanism, making the architecture extensible when replacing the mechanism component without reengineering other parts of trust components and consequently producing large overhead costs. The separation of concerns with

well-defined interfaces used for communication between decomposed components also provides benefits to capture the characteristics of the proposed mechanism in highly dynamic environments due to various cheating behaviors captured. By properly designing the relations of these components, the trust systems with the proposed mechanism's capabilities are expected to be scalable in terms of interacting raters and to achieve decentralization to discourage raters from cheating in fully distributed environments such as SOC.

6. Conclusion

This survey presents the research direction towards solving the problems of the Reputation-Based Trust mechanism (RBT) in SOC: (1) a biased reputation accumulated from unfair ratings given by raters (i.e., service users that rationally provide ratings to other services); and (2) the lack of a suitable distributed architecture to support the proposed mechanisms for solving cheating behavior, specifically in terms of optimized overhead costs regarding the four interfacing metrics: extensibility, scalability, decentralization, and performance quality attributes. The current literature [23] [35] [56] [29] [65] [69] [16] [42] focuses on the development of mechanisms to help the RBT ensure a robust reputation, while only a few studies [59] [62] [70] have investigated the overhead costs incurred by these proposed mechanisms when they are integrated with original trust systems. Based on the analysis, there are limitations in the mechanisms proposed in the current literature and further improvement is required for: (1) a well-proven preventive mechanism to support the prevention of cheating behavior, especially when the majority raters are dishonest, (2) a proper integration technique, such as a loosely coupled component-based approach [50], to ensure the integration process of such a mechanism with the trust system is efficient, based on interfacing metrics.

References

[1]. Aberer, K. and Despotovic, Z. 2001. Managing Trust in a Peer-2-Peer Information System. Proceedings of the 10th International Conference on Information and Knowledge Management, Atlanta, Georgia, USA, pp. 310-317.

[2]. Artz, D. and Gil, Y. 2007. A Survey of Trust in Computer Science and the Semantic Web. Web Semant 5(2): 58-71.

[3]. Atrey, P. K., Hossain, M. A. and Saddik, A. E. 2008. Association Based Dynamic Computation of Reputation in Web Services. Journal of Web and Grid Services 4(2): 169-188.

[4]. Brandenburger, A. 2007. Cooperative Game Theory, Characteristic Functions, Allocations, Marginal Contribution.

[5]. Braynov, S. and Sandholm, T. 2002. Incentive Compatible Mechanism for Trust Revelation. Proceedings of the 1st International Joint Conference on Autonomous Agents and Multi Agent Systems, Italy, pp. 310-311.

[6]. Chen, B. and Chan M. C. 2010. Mobicent: a Credit-based Incentive System for Disruption Tolerant Network. Proceedings of the 29th IEEE Conference on Computer Communications (INFOCOM '10), San Diego, CA, USA, pp. 875-883.

[7]. Chen, M. and Singh, J.P. 2001, Computing and Using Reputations for Internet Ratings. Proceedings of the 3rd ACM Conference on Electronic Commerce, pp. 154-162.

[8]. Chen, T. and Zhong, S. 2010. Inpac: an enforceable incentive scheme for wireless networks using network coding. Proceedings of the 29th IEEE Conference on Computer Communications (INFOCOM '10), San Diego, CA, USA, pp. 1828-1836.

[9]. Chen, Z., Liang-Tien, C., Silverajan, B. and Bu-Sung, L. 2003. UX - An Architecture Providing QoS-Aware and Federated Support for UDDI. Proceedings of International Conference on Web Services (ICWS), pp. 171-176.

[10]. Clemen, R. T. 2002. Incentive Contracts and Strictly Proper Scoring Rules. Test 11(1): 167-189.

[11]. Damiani, E., di Vimercati, D., Paraboschi, S., Samarati, P. and Violante, F. 2003. A Reputation-based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 207-216.

[12]. Dasgupta, P. Trust as a Commodity. 1990. Trust: Making and Breaking Cooperative Relations. Gambetta, D (Ed.), Basil Blackwell. Oxford, 2000.

[13]. Day, J. and Deters, R. Selecting the Best Web Service. 2004. Proceedings of the 14th Annual IBM Centers for Advanced Studies Conference, pp. 293-307.

[14]. Dellarocas, C. 2002. Goodwill Hunting: An Economically Efficient Online Feedback Mechanism for Environments with Variable Product Quality. Proceedings of the Workshop on Agent-Mediated Electronic Commerce, London, UK, pp. 238-252.

[15]. Elliott, C. 2006. Hotel Reviews Online: In Bed with Hope, Half-Truths and Hype. The New York Times.

http://ehotelier.com/hospitality-news/item.php?id=A7571_0_11_0_M Last access on 4th August 2011.

[16]. Gerding, E., Larson, K. and Jennings, N. 2009. Mechanism Design for Eliciting Probabilistic Estimates from Multiple Suppliers with Unknown Costs and Limited Precision. Proceedings of the 11th International Workshop on Agent-Mediated Electronic Commerce, pp. II 1-124.

[17]. Gintis, H. 2000. Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Interaction. Princeton University Press.

[18]. Harmon, A. 2004. Amazon Glitch Unmasks War of Reviewers. The New York Times. http://www.nytimes.com/2004/02/14/us/amazon-glitch-unmasks-war-of-reviewers.html Last access on 4th August 2011.

[19]. Hennig-Thurau, T., Gwinner, K. P., Walsh, G. and Gremler, D. D. 2004. Electronic Word-of-Mouth via Consumer-Opinion Platforms: What Motivates Consumers to Articulate Themselves on the Internet? Journal of Interacting Marketing 18 (1), 38-52.

[20]. Hu, N., Pavlou, P. and Zhang, J., 2006. Can Online Reviews Reveal a Product's True Quality? Proceedings of the ACM Conference on Electronic Commerce, pp. 324-330.

[21]. Johnson, S., Pratt, J. and Zeckhauser, R. 1990. Efficiency Despite Mutually Payoff-Relevant Private Information: The Finite Case. Econometrica 58(1): 873-900.

[22]. Jøsang, A., Ismail, R., and Boyd, C. 2007. A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems 43(2): 618-644.

[23]. Jurca, R. and Faltings, B. 2003. An Incentive-Compatible Reputation Mechanism. Proceedings of the IEEE Conference on E-Commerce, Newport Beach, CA, USA.

[24]. Jurca, R. and Faltings, B. 2004. CONFESS: An Incentive Compatible Reputation Mechanism for the Online Hotel Booking Industry. Proceedings of the IEEE Conference on E-Commerce, San Diego, CA, USA, pp. 205-212.

[25]. Jurca, R. and Faltings, B. 2007. Collusion-resistant, incentive-compatible feedback payments. Proceedings of ACM Conference on Electronic Commerce, pp. 200-209.

[26]. Jurca, R. and Faltings, B. 2009. Mechanisms for Making Crowds Truthful. Journal of Artificial Intelligence Research 34(1): 209-253.

[27]. Kamvar, S.D., Schlosser, M.T. and Garcia-Molina, H. 2003. The Eigentrust Algorithm for Reputation Management in P2P Networks. Proceedings of the 12th International Conference on World Wide Web, Budapest, Hungary, pp. 640-651.

[28]. Kandori, M. and Matsushima, H. 1998. Private Observation, Communication and Collusion. Econometrica 66(3): 627-652.

[29]. Karta, K. 2005. An Investigation on Personalized Collaborative Filtering for Web Service Selection. Master's Thesis, The University of Western Australia.

[30]. Keates, N. 2007. Deconstructing TripAdvisor. The Wall Street Journal, pp. W1. http://online.wsj.com/article/SB118065569116920710.html Last access on 4th August 2011.

[31]. Klein, M., Plakosh, D. and Wallnau, K. 2008. Using the Vickrey-Clarke-Groves Auction Mechanism for Enhanced Bandwidth Allocation in Tactical Data Networks. Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2008-TR-004.

[32]. Kagel, J.H. and Roth, A.E. 1995. Handbook of Experimental Economics. Princeton University Press.

[33]. Li, Z., Su, S. and Yang, F. 2007. WSrep: A Novel Reputation Model for Web Services Selection. N.T. Nguyen et al. (Eds.), pp. 199-208.

[34]. Liu, J. and Issarny, V. 2007. An Incentive Compatible Reputation Mechanism for Ubiquitous Computing Environments. International Journal of Information Security 6(5): 297-311.

[35]. Liu, Y., Ngu, A. and Zheng, L. 2004. QoS Computation and Policing in Dynamic Web Service Selection. Proceedings of the 13th World Wide Web Conference, pp. 66-73.

[36]. Liu, Y., Yang, Y. and Sun, Y. L. 2008. Detection of Collusion Behaviors in Online Reputation Systems. Proceedings of Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, pp. 1368-1372.

[37]. Malik, Z. and Bouguettaya, A. 2009. A. Rater Credibility Assessment in Web Services Interactions. World Wide Web Journal 12 (1): 3-25.

[38]. Maximilien, E. M. and Singh, M. P. 2005. Multiagent System for Dynamic Web Services Selection. Proceedings of the 1st Workshop on Service-Oriented Computing and Agent-Based Engineering (SOCABE at AAMAS), Utrecht, Netherlands, pp. 25-29.

[39]. Miller, J. 2003. Game Theory at Work: How to Use Game Theory to Outthink and Outmaneuver Your Competition. McGraw-Hill.

[40]. Miller, N., Resnick, P. and Zeckhauser, R. 2005. Elicit Honest Feedback: The Peer-Prediction method. Management Science 51(1): 1359 – 1373.

[41]. Moscibroda, T. and Schmid, S. 2009. On mechanism design without payments for throughput maximization. Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM '09), Rio de Janeiro, Brazil.

[42]. Nguyen, H. T., Zhao W. and Yang, J. 2010. A Trust and Reputation Model Based on Bayesian Network for Web Services. Proceedings of the 8th IEEE International Conference on Web Services (ICWS), Miami, Florida, USA, pp. 251-258.

[43]. OASIS: UDDI (V3.0.2). 2004. http://www.uddi.org/pubs/uddi_v3.htm Last access on 4th August 2011.

[44]. Osborne, M. and Rubinstein, A. 1994. A Course in Game Theory. MIT Press.

[45]. Park, J. and Schaar M. V. D. 2010. Pricing and Incentives in Peer-to-Peer Networks. Proceedings of the 29th IEEE Conference on Computer Communications (INFOCOM '10), San Diego, CA, USA.

[46]. Park, S., Lui, L. Pu, C., Srivatsa, M. and Zhang, J. 2005. Resilient Trust Management for Web Service Integration. Proceedings of the 3th International Conference on Web Services, pp. 499-506.

[47]. Resnick, P. and Zeckhauser, R. 2002. Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. M.R. Baye (Ed.), The Economics of the Internet and E-Commerce, volume 11 of Advances in Applied Microeconomics. Elsevier Science, pp. 127-157.

[48]. Sen, S. and Sajja, N., 2002. Robustness of Reputation-based Trust: Boolean Case. Proceedings of the 1st International Joint Conference on Autonomous agents and multiagent systems, pp. 288-293.

[49]. Shetty, S., Padala, P. and Frank, M.P. 2003. A Survey of Market-Based Approaches to Distributed Computing. Technical Report Number: TR03013.

[50]. Sicard, S., Boyer, F. and Palma, N.D. 2008. Using Components for Architecture-Based Management: the Self-repair Case. Proceedings of the 30th International Conference on Software Engineering, Leipzig, Germany, pp. 101-110.

[51]. Spanoudakis, G. and LoPresti, S. 2009. Web Service Trust: Towards a Dynamic Assessment Framework. Proceedings of the International Conference on Availability, Reliability and Security, pp. 33-40.

[52]. Straffin, P. D. 1993. Game Theory and Strategy. The Mathematical Association of America.

[53]. Talwar, A., Jurca, R. and Faltings, B. 2007. Understanding User Behavior in Online Feedback Reporting. Proceedings of the ACM Conference on Electronic Commerce. San Diego, USA, pp. 134-142.

[54]. Tan, L., Chi, C-H. and Deng, J. 2008. Quantifying Trust Based on Service Level Agreement for Software as a Service. Proceedings of the 32nd Annual IEEE International Computer Software and Applications Conference, pp. 116-119.

[55]. Truong, H. L., Samborski, R. and Fahringer, T. 2006. Towards a Framework for Monitoring and Analyzing QoS Metrics of Grid Services. Proceedings of the 2nd IEEE International Conference on e-Science and Grid Computing, Amsterdam, Netherlands, pp. 65.

[56]. Vu, L-H., Hauswirth, M. and Aberer, K. 2005. Towards P2P-based Semantic Web Service Discovery with QoS Support. Proceedings of Business Process Management Workshops, pp.18-31.

[57]. Wang, P., Chao, K., Lo, C. and Li, Y. 2008. QoS-Aware Service Selection under Consumer's Reputation. Proceedings of the IEEE International Conference on e-Business Engineering, pp. 627 – 632.

[58]. Wang, Y. and Vassileva, J. 2007. Toward Trust and Reputation Based Web Service Selection: A Survey. International Transactions on Systems Science and Applications 3(2): 118–132.

[59]. Wang, Y., Hori, Y. and Sakurai, K. 2008. Characterizing Economic and Social Properties of Trust and Reputation Systems in P2P Environment. Journal of Computer Science and Technology 23(1): 129-140.

[60]. Wichart, R., Robinson, R., Indulska, J. and Jøsang, A. 2005. SuperstringRep: Reputation-enhanced Service Discovery. Proceedings of the 28th Australian Conference on Computer Science, pp. 49-57.

[61]. Withby, A., Jøsang, A. and Indulska, J. 2004. Filtering Out Unfair Ratings in Bayesian Reputation Systems. Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi Agent Systems, New York, USA, pp. 106-117.

[62]. Witkowski, J. 2009. Elicit Honest Reputation Feedback in a Markov Setting. Proceeding of the 21st International Joint Conference on Uncertainty in Artificial Intelligence (IJCAI'09), Pasadena, California, USA, pp. 330-335.

[63]. Witkowski, J. and Parkes D. C., 2011. Peer Prediction with Private Beliefs. Proceedings of the 1st Workshop on Social Computing and User Generated Content, pp. 1-5.

[64]. Xiong, L. and Liu, L. 2004. PeerTrust: Supporting Reputation-Based Trust for Peer-

to-Peer Electronic Communities. Knowledge and Data Engineering, 16(7): 843-857.

[65]. Yang, M., Feng, Q., Dai, Y. and Zhang, Z. 2007. A Multi-Dimensional Reputation System Combined with Trust and Incentive Mechanism in P2P File Sharing Systems. Proceedings of the 27th International Conference on Distributed Computing Systems Workshops, Toronto, Canada, pp 29.

[66]. Yang, Y., Feng, Q., Sun, Y. and Dai, Y. 2008. RepTrap: A Novel Attack on Feedback-based Reputation Systems. Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, Istanbul, Turkey, pp. 1-11.

[67]. Yang, Y., Sun, Y., Kay, S. and Yang, Q. 2009. Defending Online Reputation Systems against Collaborative Unfair Raters through Signal modeling and Trust. Proceedings of the 24th ACM Symposium on Applied Computing, pp. 1308.

[68]. Yin, K., Zhou, B., Zhang, S. and Chen, Y. 2008. An Effective Approach to Select Trustable Web Services. : Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-6.

[69]. Zhang, G., Zhang, H. and Wang, Z. 2009. A QoS-Based Web Services Selection Method for Dynamic Web Service Composition. Proceedings of the 1st International Workshop on Education Technology and Computer Science, Wuhan, Hubei, China, pp. 832-835.

[70]. Zhao, H., Yang, X. and Li, X. 2011. An Incentive Mechanism to Reinforce Truthful Reports in Reputation Systems. Journal of Network and Computer Applications (JNCA), Elsevier, 2011 (in press).

[71]. Zohar, A. and Rosenschein, J. S. 2008. Mechanisms for Information Elicitation. Journal of Artificial Intelligence Research 172(16): 1917-1939.