A Robust Reputation System for the Grid

Jianshu Weng, Chunyan Miao and Angela Goh
School of Computer Engineering, NTU
{WENG0004,ASCYMiao,ASESGoh}@ntu.edu.sg
February 27, 2006
Abstract

Typically, users of the Grid (i.e. resource consumers) identify resources to submit their tasks based on the resources’ capabilities, e.g. processor type, memory size, etc. However, the reliability of the users who manage the resources (i.e. resource providers) is usually unknown to the consumers, e.g. one provider may intentionally drop a consumer’s submitted task in favor of another consumer’s task since the latter can pay more. Therefore, there is a risk for consumers that their submitted tasks may fail. Establishing reputation systems is a good alternative to manage this risk [1]. However, existing work regarding the reputation systems in the Grid mainly focuses on methods to calculate reputation to model resource providers’ reliability. They do not effectively mitigate the influence of inaccurate testimonies and malicious referrers, which are common phenomena in real environments. Against this background, this paper proposes a robust reputation system that has components to mitigate the influence of the inaccurate testimonies and malicious referrers. Experimental results show that the proposed system is efficient in mitigating the influence of these inaccurate testimonies and malicious referrers.
1 Introduction

The real problem underlying the Grid is resource sharing [6]. Typically, users of the Grid (i.e. resource consumers) identify resources to submit tasks based on the resources' capabilities, e.g. processor type, memory size, etc. For example, the Monitoring and Directory Service in Globus\(^1\) provides users the information about available resources' capabilities to facilitate the resource selection in the Grid. However, the reliability of the resource providers who manage the resources are unknown to the resource consumers. For example, a resource consumer submits its task to a resource provider that fits its resource requirement and cost requirement. However, the provider intentionally drop the consumer’s submitted task in favor of another consumer’s task as the latter can pay more. Therefore, there is a risk for the consumers that their submitted tasks may fail.

Establishing reputation systems is a good alternative to manage this risk [1]. In reputation systems, each consumer records personal experience with the resource provider after utilizing the resource. The provider’s reputation can be evaluated based on the provider’s successful resource provisions\(^2\) recorded in the personal experience. The reputation is basically an indicator of reliability, i.e. how the provider is likely to behave in future. A rational consumer generally opts for the providers with higher reputations.

Due to certain reasons, e.g. incomplete or even no personal experience, one’s evaluation of a provider’s reputation based on personal experience may not reflect the provider’s reliability accurately. So one consumer would ask others about their personal experience with the same provider in order to calculate a reputation that reflects the provider’s reliability more accurately. Due to the same reasons, the testimonies may not be accurate either. Even worse, some malicious consumers would intentionally give inaccurate testimonies for or against certain providers. For example, consumer \(R\) is now evaluating provider \(P\)’s reputation. \(R\) queries consumer \(A\) and \(B\) for their testimonies on \(P\). However, consumer \(A\), \(B\), and \(P\) are part of the same

\(^1\)Globus: http://www.globus.org.
\(^2\)A successful resource provision means that the provider does complete the task by providing the resource as it claims to deliver.
conspiracy, $A$ and $B$ intentionally give testimonies that $P$ never fails regardless of the truth that $P$ always fails. This will result in $P$’s exaggerated positive reputation, which leads to $R$’s wrong decision to submit tasks to $P$. Therefore, the reputation systems must be able to mitigate the influence of inaccurate testimonies.

It is possible that one asks for testimonies from some consumers that have no personal experience with the provider. To increase the chance of finding testimonies, those consumers are usually asked to recommend some other consumers. This introduces the possibility of malicious consumers (i.e. referrers) recommending the requesting consumer to “bad” referents. For example, consumer $R$ is now evaluating provider $P$’s reputation. $R$ first asks consumer $A$ and $B$ for testimonies. Consumer $A$, $B$, $C$, $D$, and $P$ have formed a clique. $A$ and $B$ intentionally refer $R$ to $C$ and $D$. Then $C$ and $D$ intentionally give testimonies that $P$ never fails though $P$ always fails, which subsequently results in $R$’s wrong decision again. Thus, the reputation systems must also be able to mitigate the influence of malicious referrers.

To the best of our knowledge, there is very little work that studies the reputation in the Grid [1]. Generally speaking, existing work mainly focuses on how a consumer can calculate reputations to model the providers’ reliability. They do not effectively mitigate the influence of the inaccurate testimonies and malicious referrers. Hence, to meet the aforementioned requirements, a reputation system with the ability to mitigate the influence of the inaccurate testimonies and malicious referrers is proposed in this paper.

The remainder of this paper is organized as follows. Section 2 defines some terms that are used throughout this paper. Section 3 discusses the proposed system’s reputation modeling component. Section 4 presents the component to mitigate the influence of inaccurate testimonies, while Section 5 presents the component to mitigate the influence of the malicious referrers. Experimental results are presented in Section 6 to show the efficiency of the proposed system. A brief review of related work is given in Section 7, followed by the conclusions and future work in Section 8.
2 Terms

In this section, some terms that will be used throughout the rest of this paper are defined.

2.1 Peers

In the Grid, there are providers who are capable of providing resources to solve users’ tasks. The tasks to be solved can be of any type, e.g. computation, storing information, etc. Users who utilize the resources to solve tasks are termed consumers.

Each consumer can take more than one role. When calculating providers’ reputations, a consumer can be the testimony requester asking for testimonies from others. It can also be the witnesses that give testimonies to others. Similarly, a consumer can be the referral initiator asking for referent, from whom it can contact further for testimonies. It can also be the referrer who refers others to a particular initiator, or the referent if it is referred by others. In the rest of this paper, each consumer is termed as a peer when it is not necessary to discriminate the role it takes.

In the rest of this paper, $P = \{P_1, \ldots, P_n\}$ is used to denote the set of providers, and $C = \{C_1, \ldots, C_m\}$ is used to denote the set of peers, where $n$ and $m$ are the numbers of providers and peers. Without loss of generality, the presentation of the proposed system is from the perspective of a particular set of provider and peer $P_n$ and $C_s$ in this paper.

2.2 Reputation, Trustworthiness, and Meta Trustworthiness

A provider’s reputation captures its reliability in providing resources to solve problems. Reputation is a local measurement. That is to say, same provider may have diverse evaluations of reputation from the perspective of different peers\(^3\). This is reasonable since different peers may have different experience with same provider. In the rest of this paper, $r_{s,n}$ is used to represent

\(^3\)In contrast, global measurement means that same provider has identical evaluation of reputation from the perspective of all peers.
C_s’s local evaluation of P_n’s reputation without aggregating others’ testimonies, and R_{s,n} is used to represent peer C_s’s evaluation of provider P_n’s reputation after testimonies aggregation. When contacted by other peers for testimonies, C_s returns r_{s,n}, but not R_{s,n}, i.e. C_s never propagates what it hears from others.

A peer’s credibility in giving testimonies on providers’ reputations is termed as its trustworthiness. As a peer’s local evaluations of providers’ reputations may not reflect the providers’ reliability accurately, other peers’ testimonies are sought hoping that they can be aggregated to derive more accurate evaluations of the providers’ reputations. In this sense, trustworthiness can be interpreted by following Barber’s definition [2] which defines trust to be the expectation of one’s technically competent role performance. Following this definition, provider’s reputation and peer’s meta trustworthiness (to be discussed in next paragraph) can also be thought as particular types of trustworthiness. They are labeled with different notations in order to avoid overusing the same term. It is noted that trustworthiness is also a local measurement. In the rest of this paper, peer C_s’s evaluation of C_t’s trustworthiness is denoted by T_{s,t}.

A peer’s credibility in referring other peers is termed as its meta trustworthiness. Meta trustworthiness is also a local measurement, and peer C_s’s evaluation of C_t’s meta trustworthiness is denoted as MT_{s,t} hereafter.

3 Modeling of Reputation

In the proposed system, Beta reputation system [9] is adopted to model providers’ reputations.

With the Beta reputation system, each consumer is allowed to give a feedback for the provider after a session of resource utilization is cleared. The consumer gives a positive feedback of “1” to the provider if the provider did not fail. Otherwise it gives a negative feedback of “0”. Consumer C_s’s feedback for the provider P_n after a session of resource utilization t can be expressed in vector notation as:
Before a new session of resource utilization, \( C_s \) derives its local evaluation of \( P_n \)'s reputation based on the summary of its past feedbacks for \( P_n \). The summary of the feedbacks can also be represented in vector notation as (2), where \( T \) is the new session number.

\[
A^T_{s,n} = \left[ \frac{P}{N} \right] = \sum_{t=T-W+1}^{T} \lambda^{T-t} \cdot a^t_{s,n}, \ (T - t) \leq W. \tag{2}
\]

In (2), the meaning of \( W \) is that consumer \( C_s \) only records its feedbacks for \( P_n \) within a window of size \( W \). And \( \lambda \) is a decay factor, which controls the rate at which \( P_n \)'s past behavior is forgotten. The windowed and decayed feedback summary is necessary to capture the observation that consumers generally “cares” more about the providers’ recent behavior and “forgets” their past behavior [1, 7].

Beta Reputation system assumes that \( P_n \)'s reliability can be modeled by a Beta distribution, whose probability density function (PDF) is given by:

\[
\text{beta}(Pr | \alpha, \beta) = \frac{1}{B(\alpha, \beta)} Pr^{\alpha-1} (1 - Pr)^{\beta-1},
\]

\[
0 < Pr < 1, \alpha \geq 1, \beta \geq 1 \tag{3}
\]

where \( B(\alpha, \beta) \) is the Beta function. The two parameters of the Beta distribution that models \( P_n \)'s reliability are given by \( \alpha = P + 1, \beta = N + 1 \). Then \( C_n \) derives its local evaluation of \( P_n \)' reputation as the expectation value of the Beta distribution, which is given by:

\[
r_{s,n} = E(Pr) = \frac{\alpha}{\alpha + \beta} \tag{4}
\]

\( r_{s,n} \), as the expectation value of the Beta distribution, predicts the probability that \( P_n \) will not fail. If \( C_s \) has no personal experience with the provider \( P_n \) before, \( P = N = 0 \), \( \alpha \) and \( \beta \) are set to 1 correspondingly, which makes
\( r_{s,n} = 0.5 \). This is interpreted that \( P_n \) has equal probabilities of failing or not. As \( C_s \) obtains new personal experience with \( P_n \), the value of \( P \) and \( N \) are updated, and \( r_{s,n} \) is updated subsequently.

4 Modeling of Trustworthiness

In the proposed system, peers are allowed to aggregate others’ testimonies. However, sometimes the testimonies may be inaccurate. The reason might be the witnesses have incomplete information about the providers, or the witnesses intentionally give inaccurate testimonies for or against some certain providers. This section discusses the aggregation of testimonies and the modeling of trustworthiness, which is used to mitigate the influence of inaccurate testimonies.

4.1 Aggregating Testimonies

In the proposed system, the testimonies aggregation is implemented as a Weighted Majority Algorithm [10]. The original idea of Weighted Majority Algorithm (WMA) is to build a master algorithm that makes predictions for a given problem based on the predictions of a pool of algorithms. Each algorithm in the pool is assigned a weight, which controls its strength in influencing the master algorithm. Then after each new prediction, master algorithm adjusts the weights for the algorithms in the pool based on the distances between the predictions given by the algorithms and its own posterior experience with the problem.

For the case of testimony aggregation, the problem is to predict provider \( P_n \) ’s reputation, and the counterpart of the master algorithm is \( C_s \). Other peers’ testimonies can be seen as predictions of the algorithms in the pool, and \( C_s \)’s local evaluations of peers’ trustworthiness take the role of weights. With WMA, \( C_s \) can derive the testimonies aggregation as a weighted sum of the testimonies:

\[
R'_{s,n} = \frac{\sum_{x \in W_{s,n}} T_{s,x} \cdot r_{x,n}}{\sum_{x \in W_{s,n}} T_{s,x}}
\] (5)
Here $W_{s,n}$ is the set of witnesses. $r_{x,n}$ is the testimony given by witness $C_x$. $T_{s,x}$ is $C_s$’s evaluation of witness $C_x$’s trustworthiness. The aggregation $R'_{s,n}$ is further aggregated with $C_s$’s local evaluation of $P_n$’s reputation $r_{s,n}$ to derive a more accurate evaluation of $P_n$’s reputation:

$$R_{s,n} = conf \cdot r_{s,n} + (1 - conf) \cdot R'_{s,n}$$

(6)

$conf$ is $C_s$’s confidence about its local evaluation of $P_n$’s reputation, which is defined as:

$$conf = w/W$$

(7)

where $W$ is the pre-selected window size of the Beta Reputation system (as in (2)) and $w$ is the number of personal experience with $P_n$ when calculating $P_n$’s reputation. If $C_s$ has no personal experience with $P_n$, $w = 0$, which makes evaluation of $P_n$’s reputation solely based on the testimonies.

4.2 Update of Peers’ Trustworthiness

$C_s$ obtains a new personal experience with $P_n$ after utilizing the resource managed by the latter, based on which it updates its local evaluation of $P_n$’s reputation. Since $P_n$’s reputation is seen as the problem in the WMA, $C_s$’s updated local evaluation of $P_n$’s reputation can be seen as the posterior experience with the problem.

If a witness $C_x$’s testimony is far from the posterior experience, possibly it is giving inaccurate testimony. Consequently, $C_x$ must be assigned a smaller weight when aggregating testimonies next time. $r'_{s,n}$ denotes $C_s$’s updated local evaluation of $P_n$’s reputation. $C_n$ updates the trustworthiness of the witness $C_x$ as [10]:

$$T'_{s,x} = (1 - (1 - conf) \cdot \alpha) \cdot |r_{x,n} - r'_{s,n}| \cdot T_{s,x}$$

(8)

where $r_{x,n}$ is $C_x$’s testimony, and $T_{s,x}$ is $C_s$’s original evaluation of $C_x$’s trustworthiness. $\alpha$ is a fixed constant, which is always in the range $0 \leq \alpha < 1$. 
When \( C_s \) becomes more confident about its local evaluation of the \( P_n \)'s reputation, it is more confident about whether a testimony is accurate. So \( T_{s,x} \) receives a update of more significant magnitude with a larger \( conf \).

Initially, \( T_{s,x} \) is set to 1, which means \( C_s \) assumes full trustworthiness of \( C_x \) before their first experience. Then \( T_{s,x} \) is updated every time \( C_x \) gives a testimony.

5 Modeling of Meta Trustworthiness

The last section discusses the evaluation of provider’s reputation with the testimonies aggregation. But it does not answer the question how testimonies are discovered. In the proposed system, a referral-based process [13] is adapted to discover testimonies. To facilitate the testimonies discovery, each peer maintains a set of direct neighbors. A peer contacts directly its direct neighbors for testimonies. It also recommends others to its direct neighbors if it has no testimonies to give when it is contacted for testimonies.

One may argue that a central directory can be established to maintain a list of all existing peers, so that \( C_s \) can directly contact all the existing peer for testimonies. The main concern leading to not using this strategy is that the central service may become a single-point failure. Moreover, maintaining the list requires extra overhead as peers may keep entering and exiting the Grid.

5.1 Referral-based Testimonies Discovery

\( C_s \) contacts its direct neighbors for testimonies first. A direct neighbor of \( C_s \), say \( C_d \), returns its testimony on the provider’s reputation to \( C_s \) if it is a witness, i.e. it has experience with the provider before.

If \( C_d \) has no testimony to give, it generates referrals for \( C_s \). Each referral contains the contact information of one of \( C_d \)'s direct neighbors and its evaluation of this referent’s trustworthiness. \( C_d \) may not tell the truth about the referent’s trustworthiness. Hence, the referent’s trustworthiness reported by \( C_d \) is to be discounted with \( C_d \)'s meta trustworthiness, which captures its
capability in referring other peers. Then $C_s$ applies a probabilistic strategy to determine whether to contact a particular referent for further testimonies discovery: it contacts a referent $C_m$ at next step with a probability $MT_{s,d} \cdot T_{d,m}$, and does not contact $C_m$ with a probability $1 - MT_{s,d} \cdot T_{d,m}$. $T_{d,m}$ is $C_d$’s reported evaluation of $C_m$’s trustworthiness, and $MT_{s,d}$ is $C_s$’s evaluation of $C_d$’s meta trustworthiness. Then every contacted peer carries out the same operations as $C_d$ does. $C_s$ contacts a referent only once for same provider’s reputation even the latter is referred to by different referrers more than one time.

The probabilistic strategy applied during the course of witness discovery has the following advantages:

- Compared with the strategy of contacting all the referents, it helps to reduce the network load.
- Peers with higher trustworthiness have a higher probability to be contacted. This helps $C_s$ to discover more credible testimonies.
- Nevertheless, peers with lower trustworthiness may also be contacted though with lower probabilities. This gives those peers opportunities to interact with $C_s$, which helps to promote $C_s$’s evaluation of their trustworthiness.

A path starting from $C_s$ and connecting the series of contacted referents forms a referral chain. The witness is always at the end of a referral chain if a witness can be discovered by following the referral chain. An upper bound ($U$) is applied on the referral chain length. $C_s$ stops contacting any referent if the referral chain length $> U$ no matter whether testimonies have been discovered or not. According to the small world observation, $U$ is generally small, e.g. $U < 6$.

Example of referral chains are shown in Figure 1, in which $C_1$ is discovering testimonies on provider $P_1$. $C_5$ and $C_6$ are two witnesses discovered. The two corresponding referral chains are $c_1 \rightarrow c_2 \rightarrow c_4 \rightarrow c_6$ and $c_1 \rightarrow c_3 \rightarrow c_5$. The outgoing edges from one peer to its referents are labeled with the probabilities that $C_1$ will contact the referents. It is noted that the edges from $C_s$ to its direct neighbors are only labeled with the direct neighbors’ trustworthiness.
This is because $C_s$ will always report its direct neighbors’ trustworthiness honestly to itself (i.e. $MT_{s,s} = 1$).

### 5.2 Update of Peers’ Meta Trustworthiness

Upon $C_s$ gaining the posterior experience with the provider after utilizing the resource, it updates the witnesses’ trustworthiness, which subsequently triggers the update of the meta trustworthiness of the peers who refers $C_s$ to the witnesses. Since $C_s$ discovers the witnesses by following the referral chain, all the peers along the referral chains contribute to the discovery of the witnesses. Therefore, meta trustworthiness of all the peers along the referral chains (excluding $C_s$ and the discovered witnesses) are to be updated. In the proposed system, the update of peers’ meta trustworthiness is carried out as a spreading activation process.

Spreading activation theory has originally been used in cognitive science [3], and has then been adapted to other fields, e.g. [14, 4]. It is about determining the energy of each node within a network with a number of interconnecting nodes. After injecting an initial activation $I^0$ into a node, the activation spreads over the whole network. If $ei(x)$ denotes the energy that a node $x$ receives, the node retains $(1 - d) \cdot ei(x)$ to update its current energy, and spreads $d \cdot ei(x)$ to the nodes it directly connects. The energy that a node $y$ receive from $x$ is determined as:

$$ ei(y) = d \cdot ei(x) \cdot \frac{E(x, y)}{\sum_{(x,s) \in OE} E(x, s)} $$

(9)
where $d$ is the spreading factor, $ei(x)$ is the energy that $x$ receives, $E(x,y)$ is the weight of the edges from node $x$ to $y$, and $OE$ is the set of node $x$’s outgoing edges. Practically, the spreading stops when the update of each node’s energy (after receiving energy) is less than a predefined threshold.

For the case of meta trustworthiness update, the counterpart of the nodes is the peers, and the energy that each peer has is basically its meta trustworthiness. The energy each peer receives during the course of update is in fact the magnitude of the update in the meta trustworthiness that each peer should undertake.

The update of peers’ meta trustworthiness is carried out along the reversed referral chain. The edges in all the referral chains are preserved in the reversed referral chains, but the directions of the edges are reversed. Figure 2 shows examples of reversed referral chains based on the referral chains in Figure 1. For example, there is a outgoing edge from Peer $C_3$ to $C_5$ in Figure 1. Correspondingly, there is a outgoing edge from $C_5$ to $C_3$ in the reversed referral chain.

During the course of meta trustworthiness update, an initial activation $I^0$ is injected into the direct referrer of the witness, i.e. the direct successor of the witness in each reversed referral chain. The quantity of $I^0$ equals to the absolute change in the witness’ trustworthiness after $C_s$ updates the witness’ trustworthiness. Since each referral chain contains no branches, the third term in the RHS of (9) is always 1. Hence the energy that spreads from one peer flows completely into its direct successor along the reversed referral chain. For this reason, the update of meta trustworthiness is in fact a partially-implemented spreading activation.
During the course of meta trustworthiness update, each peer retains \( (1 - d) \) of the energy \( (ei(x)) \) it receives to update its current meta trustworthiness, and spreads \( d \cdot ei(x) \) to its successor along the reverse referral chain. By retaining \( (1 - d) \cdot ei(x) \) to update the meta trustworthiness, each peer’s meta trustworthiness is updated as follows:

\[
MT_{s,x} = (1 - (1 - d) \cdot ei(x)) \cdot MT_{s,x}
\]  

(10)

The spreading factor \( (d) \) controls whether to penalize peers near the witnesses or to penalize peers far from the witnesses. Small values of \( d \) (e.g. \( d < 0.5 \)) tend to penalize peers close to the witness, whereas large values of \( d \) (\( d > 0.5 \)) tend to penalize peers far from the witnesses. The process to update of peers’ meta trustworthiness is summarized in Figure 3.

5.3 Updating Neighborhood

Direct neighbors play an important role in the testimonies discovery. When a peer joins the Grid, it chooses direct neighbors randomly since it has no experience with any peer in the Grid. After that, each peer gets to know more peers via the referral process. Moreover, each peer’s evaluations of other peers’ trustworthiness and meta trustworthiness keep updating as the former obtains new experience with other peers, including its direct neighbors and the peers it gets to know via referral. Some direct neighbors may become less credible either in terms of trustworthiness or meta trustworthiness. As a result, it is necessary for peers to update the neighborhoods, i.e. to replace a number of less credible direct neighbors with more credible ones.

When an instance of update starts, first of all, \( C_s \) assigns each peer (including its current direct neighbors and the peers it knows via referrals) a score as a linear combination of trustworthiness and meta trustworthiness using (11), where \( \theta \) controls whether emphasis is given to peers’ trustworthiness or meta trustworthiness.

\[
\text{score}(C_i) = \theta \cdot T_{s,i} + (1 - \theta) \cdot MT_{s,i}
\]  

(11)
Procedure 1 MTUpdate(\(C_s, C_w\))

Input:
\(C_s\): the requesting peer who is calculating the reputation of the candidate provider \(C_n\);
\(C_w\): a witness of the provider \(C_n\);
\(T_{s,w}\): \(C_s\)'s original evaluation of \(C_w\)'s trustworthiness;
\(T'_{s,w}\): \(C_s\)'s new evaluation of \(C_w\)'s trustworthiness;
\(\mathcal{R}\): the series of peers (excluding \(C_s\) and \(C_w\)) along the referral chain leading to \(C_w\), and they are sorted in the order of appearance in the reversed referral chain;
\(C_i\): a peer in \(\mathcal{R}\);
\(MT_{s,i}\): \(C_s\)'s evaluation of \(C_i\)'s meta trustworthiness;

1: \(N = \|\mathcal{R}\|\);
2: \(I^0 = |T'_{s,w} - T_{s,w}|\);
3: \(e_{i0} = I^0\);
4: \textbf{for} \(i = 1\) to \(N\) \textbf{do}
5: \(MT_{s,i} = (1 - (1 - d) \cdot e_{i-1}) \cdot MT_{s,i-1}\);
6: \(e_{i} = d \cdot e_{i-1}\);
7: \textbf{end for}

Figure 3: Meta trustworthiness update
1: discover a set of witnesses on the provider $P_n$: $W_{s,n}$;  
2: evaluate $P_n$’s reputation $R_{s,n}$ using (6);  
3: make the decision whether to utilize the resource managed by a particular provider $P_n$;  
4: if utilize the resource managed by $P_n$ then  
5: update the local evaluation of $P_n$’s reputation with the posterior experience with $P_n$;  
6: for all $C_x \in W_{s,n}$ do  
7: update $C_x$’s trustworthiness using (8);  
8: update the meta trustworthiness of the peers along the referral chain leading to $C_x$ using $MTUpdate(P_s, P_x)$;  
9: end for  
10: end if  
11: update the neighborhood if there are already $F$ sessions of resource utilization since last instance of neighborhood update.

Figure 4: Process of the Proposed System

Then the top $L$ ones with highest scores are $C_s$’s new direct neighbors, where $L$ is the number of direct neighbors each peer maintains. $L$ is usually small, i.e. $L \leq 10$, and $L$ is always kept unchanged after updates. The update is carried out periodically with certain frequency $F$, i.e. update after every $F$ sessions of resource utilization.

5.4 Summary

By putting all the components of the proposed system together, the process of the proposed system is summarized in Figure 4.

6 Experimental Study

It has already been reported in [9, 8] that Beta Reputation system can capture providers’ reliability accurately with the modeling of reputations.
Parameter | Description | Value
---|---|---
$L$ | Number of direct neighbors each peer maintains | 5
$U$ | Bound of referral chain length | 5
$W$ | Window size in (2) | 10
$\lambda$ | Forgetting factor in (2) | 0.9
$\alpha$ | The update constant in (8) | 0.5
$d$ | Spreading factor in (10) | 0.2
$\theta$ | The weighting factor in (11) | 0.8
$F$ | Neighborhood Update Frequency | 5

Table 1: The parameters of the testbed

Hence, the main purpose of the experiments is to study the proposed system’s efficiency in mitigating the influence of the inaccurate testimonies and malicious referrers. The experiments were based on a simulation testbed, which consisted of a set of providers ($\mathcal{P}$) and a set of consumers ($\mathcal{C}$). $|\mathcal{P}| = 10$ and $|\mathcal{C}| = 40$.

In the experiments, each consumer generated a random set of 50 tasks to be completed. As we are only interested in studying the proposed system’s efficiency, each task does not contain any concrete activities. For each task, all the providers are able to provide resource to solve it. With the proposed system deployed, each consumer submits the task to the provider with highest reputation. If the selected provider fails to complete the task, the consumer submits the task to the provider with the second highest reputation. It repeats the above process until the task is completed or all providers fail.

Each provider’s reliability is controlled by its loyalty, which is unknown to the consumers. The loyalty of a provider controls the intrinsic probability that provider will not fail. In the testbed, there are three providers with very low loyalties (around 0.1), three low (around 0.3), three high (around 0.6), and only one high (around 0.9). Providers’ loyalties are changing due to many reasons, e.g. the current workload, the cost to solve a task, etc. The change of each peer’s loyalty was simulated as a normal distribution with a mean of 0 and standard variance of 0.05. The other parameters of the testbed were set as Table 1 shows.
6.1 Comparison with Other System

Among all the existing work, the most similar to the proposed system is the work by Whitby et. al [12]. It is also based on Beta Reputation system. Instead of giving each witnesses a weight, it applies an iterative filtering methods to mitigate the influence of inaccurate testimonies. The filtering method analyzes each testimony against the aggregated testimonies directly, and discards a testimony if it is thought to be an inaccurate testimony. This method aggregates all the available testimonies first, and then filters each testimony by testing whether the testimony is outside the $q$ quantile and $(1-q)$ quantile of the Beta Distribution that models the testimonies aggregation. If the test is positive, the testimony is considered as an inaccurate testimony and is discarded. Then the remaining testimonies are aggregated and filtered again. This process is iterated until no more testimony can be discarded. The efficiency of the method in mitigating the influence of inaccurate testimonies depends on the value of $q$. For the comparison, $q$ was set as 0.01 which is a good choice as reported in [12]. In addition, a similar process of testimonies discovery was implemented, with a strategy of contacting all referents.

6.2 Individual Inaccurate Testimony

The influence of individual inaccurate testimony was studied. Individual inaccurate testimony means that each peer provides inaccurate testimonies individually without forming a collusion. There were two types of inaccurate testimonies studied:

**Type 1:** ballot-stuffing, which peers give testimonies that the providers never fail regardless of their real experience, and

**Type 2:** bad-mouthing, which peers give testimonies that the providers always fail regardless of their real experience.

It is noted that a peer may not give inaccurate testimonies all the time. Instead, every time it provides inaccurate testimony with a certain probability.
First of all, efficiency of the proposed system in presence of different ratios of peers that gave inaccurate testimonies was studied. The probability that each peer gave inaccurate testimonies was fixed at 0.5 first, and the ratios of inaccurate peers increased from 50% to 90% with an increment 10%. To evaluate the efficiency, the average number of submissions that each peer needed to complete all its 50 tasks is measured. If the proposed system is vulnerable to the presence of inaccurate testimonies, the reputations will not capture the providers’ reliability accurately. Consequently, the peers will submit the tasks to providers with lower loyalties first, which results in the increased submissions.

The average numbers of all peers’ submissions with different ratios of peers giving inaccurate testimonies are plotted in Figure 5(a). The submissions achieved with the proposed system are labeled with “T & MT”, while the ones derived with the method discussed in Section 6.1 are labeled with “IF”. The ones labeled with “Baseline” were derived by simply aggregating testimonies as the mean of all testimonies. It can be seen that the proposed system enables the peers to finish the tasks with fewer submissions than the other two methods in all settings, though the differences are not significant.

Compared with the case that 0% of the all peers provide inaccurate testimonies, the increase in the ratio of individual peers giving inaccurate testimonies does not increase the number of submission significantly. It is shown that simply increasing the ratios of individual peers giving inaccurate testimonies has little influence on peers’ reputations.

The influence of the probability that each peer gives inaccurate testimonies was then studied. Since the ratios of individual peers giving inaccurate testimonies has little influence, the ratio of peers giving inaccurate testimonies was fixed at 50% this time. The probability of each peer giving inaccurate testimonies was set to 0.1, 0.3, 0.5 0.7, or 1.

The average numbers of each peer’s submissions in different settings are plotted in Figure 5(b). It is observed that the increased probability of individual peers giving inaccurate testimonies does increase the submissions if peers aggregate the testimonies simply as mean of all the testimonies. Nevertheless, the proposed system does mitigate the influence of inaccurate
testimonies since it manages to achieve a submission less than 68 in all settings (i.e. each peer only need an average of about 1.36 submissions to complete a task), though the difference between the proposed system and Whitby et al’s method is not significant.

6.3 Collusive Inaccurate Testimony

Then the influence of collusive inaccurate testimony was studied. It was simulated that two of the providers with very low loyalties colluded with some peers, who intentionally gave inaccurate testimonies in favor of these two colluding providers. The two providers colluded with other peers to promote their reputation in order to attract more tasks. The colluding peers always (i.e. with a probability of giving inaccurate testimony as 1) gave Type 1 inaccurate testimonies for the two colluding providers. At the same time, they gave Type 2 inaccurate testimonies for the other providers. The ratios of peers colluding with the two providers varied from 10% to 90% with an increment of 20%.

Besides measuring the number of submissions required to complete the tasks, the power of the collusion was also measured for this experiment. The power of collusion was measured as the average ratios of tasks which each peer submitted to the two colluding providers to the total number of tasks each peer had. For example, if the collusion attracted each peer to submit 40 of all the 50 tasks to one of the two colluding providers, the power of the collusion is $40/50 = 0.8$. Results in terms of power and submission are shown in Figure 5(c). It is observed in Figure 5(c) that the two colluding did attract more tasks if the testimonies were simply aggregated as mean of all the testimonies. Fortunately, the proposed mechanism manages to keep the power of collusion low via the modeling of trustworthiness. Unlike the case of individual inaccurate testimony, the proposed system outperforms Whitby et al’s method (both in terms of power of collusion and submission) obviously. With the Whitby et al’s method (as well as the Baseline method), almost all peers submitted all of their tasks to the two colluding peers (i.e. power $\approx 1$) when 90% of the peers colluded with the two
providers. Whereas, the proposed system managed to keep the power lower than 0.2 with same setting. It is thus shown that the proposed system does mitigate the influence of collusive testimonies and is much more invulnerable to collusive testimony than Whitby et al’s method.

6.4 Collusive Malicious Referrers

Influence of collusive malicious referrers was also studied in the experiments. Malicious referrers are those peers that give testimonies based on their personal experience honestly, but intentionally refer other peers to their collusion partners, who intentionally give inaccurate testimonies in favor of the providers colluding with them. Here the colluding providers were also the two providers with very low loyalties as in case of collusive inaccurate testimony. The submissions and powers when 10% of all the peers are malicious referrers in the collusion are plotted in Figure 5(d). It is observed that with only 10% malicious referrers presented in the Grid, collusive peers giving inaccurate testimonies exert more powerful influence than in cases without malicious referrers if the testimonies aggregation are simply derived as mean. For example, 30% peers giving inaccurate testimonies has a power of less than 0.1 without malicious referrers, while it has a power of about 0.35 with 10% malicious referrers. Nevertheless, the proposed system still manages to keep the power of collusion low via the modeling of trustworthiness and meta trustworthiness. Also, the difference between the efficiency (both in terms of power of collusion and submission) of the proposed system and Whitby et al’s method is obvious. It is thus shown that the proposed system does mitigate the influence of malicious referrers and is much more invulnerable to malicious referrers than Whitby et al’s method.

We also studied the influence of different ratios of malicious referrers. Similar results as the ones presented in Figure 5(d) are observed. Due to the space limitation, details are omitted here.
7 Related Work

To the best of our knowledge, there is a little work that has studied the reputation in the Grid, including [1, 7]. As the main focus of [1] is to propose an architecture for designing reputation service in the Grid, the authors did not study in detail particular reputation systems. [7] studies the reputation in the Grid and different strategies of using reputation to facilitate resource selection. However, this work derives others’ reputations solely based on personal experience and does not consider the presence of inaccurate testimonies. This may become inapplicable in cases where personal experience is not available. The feature that distinguishes the proposed system from existing work is that the proposed system takes into account the presence of inaccurate testimonies and malicious referrers. Furthermore, the system has been shown to be robust in the presence of inaccurate testimonies and malicious referrers.

In contrast to the small number of work studying reputation in the Grid, there is numerous work in reputation systems in other fields of the computer science, e.g. [9, 12, 11, 5]. Among them, the most related work to this paper is [12], which also uses Beta Reputation System to model reputation and applies an iterative filtering method to mitigate the influence of inaccurate testimonies. This work is efficient in mitigating the influence of individual inaccurate testimonies. However, as this work does not consider the collusive inaccurate testimonies and malicious referrers, it is vulnerable to the presence of collusive inaccurate testimonies and malicious referrers, which is shown by the experimental results in Section 6.3.

8 Conclusions and Future Work

Resource consumers of the Grid will take the risk that their submitted tasks may fail if they select the resource solely based on the capabilities of the resources. It is well recognized that establishing reputation systems is a good alternative to manage this risk [1]. In this paper, a reputation system for the Grid has been presented. The feature that distinguishes the proposed system
from existing work is that it is robust even in the presence of inaccurate testimonies and malicious referrers, which are common phenomena in real environment. Results of experimental studies have also been presented to support this claim.

Currently, this paper only studies the establishment of reputation system. Another important issue is how to utilize the reputation system to facilitate the resource selection in the Grid. In the experimental studies in this paper, peers always opt for the providers with higher reputations. This strategy may introduce a potential workload imbalance problem. Different strategies in making reputation-based resource selection decision are to be investigated in future work. It is also planned to implement a prototype system using existing Grid middleware such as Globus, and to study the proposed system and reputation-based resource selection in real Grid environments.

References


Submission vs. % of Peers Giving Type 1 Inaccurate Testimonies

Baseline □ T & MT □ IF

0 10 20 30 40 50 60 70 80 90
% of Peers Giving Inaccurate Testimony

Submission vs. % of Peers Giving Type 2 Inaccurate Testimonies

Baseline □ T & MT □ IF

0 10 20 30 40 50 60 70 80 90
% of Peers Giving Inaccurate Testimony

(a) Submission with different ratios of peers giving inaccurate testimonies

Submission vs. Prob. of Giving Type 1 Inaccurate Testimony

Baseline □ T & MT □ IF

0.1 0.3 0.5 0.7 0.9
Prob. of Peer giving Inaccurate Testimony

Submission vs. Prob. Of Giving Type 2 Inaccurate Testimony

Baseline □ T & MT □ IF

0.1 0.3 0.5 0.7 0.9
Prob. of Peer giving Inaccurate Testimony

(b) Submission with different probabilities of giving inaccurate testimonies

Power vs. Ratios of the Colluding Peers Giving Inaccurate Testimonies

Baseline □ T & MT □ IF

0 10 30 50 70 90
% of the Collusive Peers Giving Inaccurate Testimony

Submission vs. Ratios of the Colluding Peers Giving Inaccurate Testimonies

Baseline □ T & MT □ IF

0 10 30 50 70 90
% of the Collusive Peers Giving Inaccurate Testimony

(c) Submission and Power with collusive inaccurate testimonies

Power vs. % of Peers Giving Inaccurate Testimonies (with 10% Malicious Referrers)

Baseline □ T & MT □ IF

0.1 0.2 0.3 0.4 0.5 0.6
Prob. of Peer giving Inaccurate Testimony

Submission vs. % of Peers Giving Inaccurate Testimonies (with 10% Malicious Referrers)

Baseline □ T & MT □ IF

0 10 20 30 40
% of Collusive Peers Giving Inaccurate Testimony

(d) Submission and Power with malicious referrers

Figure 5: Experimental Results