ENHANCED RELIABLE TRUST MODEL FOR GRID COMPUTING BASED ON REPUTATION

Vivekananth.p  
Lecturer-Botho college  
Gaborone  
Botswana  
vivek.jubilant@gmail.com

Abstract
Grid computing system is a distributed environment with individual domains that share their resources. The resources must be shared without losing individual’s confidentiality and having control over their resources. One of the prevailing issues in grid security is trust relationship. Modeling trust is of great importance for the future development of grid systems. Various Reputation based trust models are coming up to address the problems in behavior conformity. This paper reviews different reputation based trust models and proposes a new model with enhanced reliability for grid computing.

Keywords
Reputation, Trust

1. INTRODUCTION:

Grid computing provides development of distributed services that integrates wide variety of resources with different quality of services. Security plays a very vital role in grid. Security challenges in grid can be classified into three categories, integration challenge, interoperability challenge, and trust relationship challenge [1].

In general security mechanisms in any environment must give protection against malicious behavior of participating members. Authorization and authentication restrict access to the resources. [1]. But with in the grid application the one who uses the resource also needs reliable and secure services. Trust and reputation address this problem.

Trust and Reputation:

When delegating a task, the initiator host must evaluate the trust on the other by considering different beliefs it can gather about the target host. Marcim Adamski et al. in [3] defines trust as “When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly, when we say that
someone is untrustworthy, we imply that that probability is low enough for us to refrain from doing so”.

Reputation can be the source of building trust. According to Abdul Rahman et al. [4] reputation is an expectation about behavior, based upon its past behavior. Reputation is what is generally said or believed about a person’s or thing’s character [2]. Therefore, reputation is a measure of trustworthiness, in the sense of reliability.

The main issues characterizing the reputation systems are the trust metric (how to model and compute the trust) and the management of reputation data how to securely and efficiently retrieve the data required for the trust computation.

There are some existing models for peer to peer net work systems, distributed systems and also for grid systems. All the models use reputation for determining the trust. These models are reviewed in this paper and the applicability of these models in enhancing the reliability for grid is analyzed. The rest of the paper is organized as follows: Section 2 surveys the previous work in the area of reputation. Section 3 presents the proposed model with its parameters. Section 4 presents conclusions.

2. **Existing models in reputation:**

Some common properties are observed in all the trust models discussed below whether they are applied to peer to peer, distributed or grid.

- Reputation trusts mechanism. (Centralized or decentralized).
- Metrics values that express the reputation of an entity: may be from –1 to 1 or 0 to 1.
- Type of reputation (positive or negative).
- Common focus (reliability).

2.1 **Peer to peer network approaches.**

In a peer-to-peer system the main concern is the identification of peers who are malicious and provide faulty services. We review three models.

Li xiong and liu present [5] a reputation-based framework. They claim that feedback values only are not enough for the calculation of trust and reputation. They introduced four more parameters such as number of transactions, the credibility of the feedbacks submitted by peers, the transaction context factor, and the community context factor. Their model is widely used in e commerce transactions.

Y. Wang and J. Vassileva [6] propose a reputation model based on Bayesian network. According to their model the peers needs are different in different situations. Their model considers two types of trust: trust in the host’s capability to provide service and trust in the host’s reliability to provide recommendations. They consider two parameters trustfulness and similarity.
Selcuk et al. suggests in [7] a reputation based trust management system in which the reliability is calculated based on previous transactions. Bit wise vector is used for storing trust values. No of feedbacks are restricted to a predefined value.

2.2 Distributed network approach:
Ayman Tajedidine et al. in [8] propose a very impressive reputation based trust model. In this approach the initiator host calculates reputation value of target host based on its previous experiences and gathered feedbacks from other hosts. The recommenders can be from the same administrative control (neighbor) or from different trusted domain (friends) or from completely strange domain (stranger).

The hierarchy of their trust is as follows.

![Trust Hierarchy Diagram]

Their model estimates credibility by considering the following parameters.

- **Similarity**: The similarity of two hosts in their reputation values and evaluation procedures.
- **Activity**: The fraction of interactions of a host with respect to all interactions.
- **Popularity**: The fraction of interactions of other host with this host, of all interactions.
- **Cooperation**: The ratio of the number of times a host responded to the total number of times it was asked for.

2.3 Grid computing environment:

In grid computing there are only few reputation based trust models. We review the following models.

F.Azzedin,M.Maheswaran [9] discuss about managing trust in grid by proposing a behavior trust management model. Trust levels are graded from a to f. Both direct and indirect trust are considered.
Gui Xiaolin, Xie Bing [10] propose a trust model based on behavior tracks. Attenuation function is incorporated for decaying factor.

Baolin Ma et al in [11] present a reputation based trusted model. Their model considers both direct feedback and feedback from other entities. Direct trust is given with more weightage than the indirect score.

Beulah kurian, Gregor von laszewki [12] provide a way for efficient resource selection. Their approach is similar to Azzedin approach [9] except for a new parameter context.

We compare the different trust models in table 1:

<table>
<thead>
<tr>
<th>Reference Parameter</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy of trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Prior-Derived Reputation</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>First Impression</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Result of Interaction</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Credibility</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Fixed decay factor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Dynamic decay factor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Similarity</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Popularity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cooperation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Number of Interactions</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Table 1. A comparison of trust models.

In Table 1 we summarize the different features incorporated in the models discussed above. We also show how our proposed model improves the reliability by incorporating all features listed in the table. The credibility factor is one of important trust metric in the calculation of reputation. The evaluation procedures vary for various models. But our model introduces an efficient way of finding out the credibility by using rank correlation.

3. Proposed model:

The proposed model uses direct trust as well as indirect trust. Higher weightage is given for direct trust. Direct trust is calculated from transactions done directly. Indirect trust is measured by getting feedbacks from entities in the same domain and also from other
domains. The credibility of the recommenders feedback is estimated by considering different parameters such as similarity, activity and specificity. Similarity is calculated by rank correlation.

**Ranking:**

Since the feedbacks are collected from different domains, there is a chance of getting biased inputs. So in this paper the concept of ranking is introduced. The feedbacks are sorted and rank is assigned. Rank correlation is calculated. If the correlation is positive then that value will be taken. Otherwise the value will be ignored. Similarity between the evaluation procedures of two entities, is estimated by using Spearman’s rank correlation. We calculate the credibility more accurately and efficiently than the existing models.

\[
\text{Similarity} = 1 - 6 \Sigma d_{ij}^2 / n (n^2 - 1)
\]

\[
\begin{align*}
\text{activity} &= \frac{\text{number interactions by recommenders}}{\text{Total number interactions by all recommenders}} \\
\text{Specificity} &= \frac{\text{Number of interactions with initiator}}{\text{Total number of interactions with all other hosts}}
\end{align*}
\]

\[
\text{Credibility} = a \times \text{similarity} + b \times \text{activity} + c \times \text{specificity} \text{ where } a > b > c \text{ and } a+b+c=1
\]

**3.1 Computation of reputation:**

Consider the scenario where entity x wants to interact with entity y to complete some task. X wants to measure the trustworthiness of y. The direct trust is calculated based upon the behavior of target entity on direct transactions. Then it inquires reputation of y from the entities in the same domain and from other domain. The reputation will be calculated from the formula given below.

\[
\text{Rep}_{y/x_k} = u \times \text{direct trust} + v \times \text{indirect 1} + w \times \text{indirect 2}
\]

Where \( u+v+w=1 \) and \( u>v>w \).

\[
\begin{align*}
\text{indirect 1} &= \frac{\Sigma \alpha_i \text{rep } y/\text{xi}}{\Sigma \alpha_i} \\
\text{indirect 2} &= \Sigma \beta_j \text{rep } y/\text{xi}
\end{align*}
\]
\[ \sum_{j \neq k} \beta_j \]

\[\alpha, \beta\] are credibility factors.

**Host Y is new to the system:**

In the case where Host Y is a new host that has just joined the system and which, consequently, has not yet interacted with any other hosts, X interacts with Y according to a predefined first impression value that X uses which may be a minimum value. Y will be assigned with un harmful resources for the initial period.

If the reputation is greater than the minimum threshold value the job will be assigned to Y. Otherwise it will be rejected. After the transaction is over the reputation table will be updated by taking the new value. The decaying factor is considered for modifying the reputation of each entity with time.

As time passes by, a host reputation with respect to other hosts typically changes to an unknown state if little or no interaction occurs between them. When a Host Z receives a request (from Host X) for reputation information about Host Y, it modifies its reputation information relative to Y by using decaying factor and then sends the result to the requesting host.

\[
\text{rep } y/z = \text{final value } + (\text{final value } - \text{initial value }) \times \gamma
\]

where \(\gamma\) depends on time. If \(t\) is the current time and \(t_0\) is the time at which the last transaction taken place then the calculation of \(\gamma\) is as follows.

\[
\gamma = 1 \text{ if } t - t_0 < 1 \text{ month } \\
\gamma = 0.75 \text{ if } 1 < t - t_0 < 2 \\
\gamma = 0.5 \text{ if } 2 < t - t_0 < 3 \\
\gamma = 0 \text{ if } t - t_0 > 3
\]

**Conclusion:**

The different reputation models are discussed and analyzed and a new reputation model for grid is proposed.

**References**


