Integrating Trust in Grid Computing Systems

Woodas W.K. Lai, Kam-Wing Ng, and Michael R. Lyu

Department of Computer Science and Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
+852-2609-8440
{wklai,kwng,lyu}@cse.cuhk.edu.hk

Abstract. A Grid computing system is a virtual resource framework. Inside the framework, resources are being shared among autonomous domains which can be geographically distributed. One primary goal of such a virtual Grid environment is to encourage domain-to-domain interactions and to increase the confidence of domains to utilize or share resources without losing control and confidentiality. To achieve this goal, a Grid computing system can be viewed more or less as a human community and thus the "trust" notion needs to be addressed. To integrate trust into a Grid, some specific issues need to be considered. In this paper, we view trust in two aspects, identity trust and behavior trust. Further, we briefly present two important issues which help in managing, evolving and interpreting trust. The two issues are grid context and trust tree structure.

1 Introduction

Trust[1] is a complex concept that has been addressed at different levels by many researchers. We classify trust into two categories: identity trust and behavior trust. Identity trust is concerned with verifying the authenticity of an entity and determining the authorizations that the entity is entitled to and is based on cryptographic techniques such as encryption and digital signatures. Behavior trust deals with a wider notion of an entity's "trustworthiness" and focuses more on the behavior of that entity. For example, a digitally signed certificate does not indicate whether the issuer is an industrial spy and a piece of digitally signed code does not show whether the code will perform some malicious actions or not.

In this paper, we will only briefly present and outline the issues that need to be considered when "trust" is being integrated into the Grid Computing Systems. We assume that each Grid service instance has a globally unique id. As stated in [2], for the OGSA architecture, every Grid service instance is assigned a globally unique name, the Grid service handle (GSH).

2 Trust and Reputation

To integrate "trust" into the Grid Computing Systems, first of all, we need to address what "trust" means.

Currently, there is a lack of consensus in the literature on the definition of trust and on what constitutes trust management. In this paper, we propose to modify the definition of trust defined in [3]:

H. Jin, Y. Pan, N. Xiao, and J. Sun (Eds.): GCC 2004, LNCS 3251, pp. 887–890, 2004.
© Springer-Verlag Berlin Heidelberg 2004

> *Trust is the firm belief in the competence of an entity to behave as expected such that this firm belief is a dynamic value associated with the entity and it is also subject to the entity's behavior and applies only within a specific context at a given time.*

That is, trust is a dynamic value between 0 and 1 inclusively. A value of 0 means very untrustworthy while a value of 1 means very trustworthy. The trust value (TV) is based on the history and is specific to a certain context. For example, entity x might be permitted to use the service s1 of entity y but is not permitted to use the service s2 of entity y at a particular time and context.

Furthermore, to establish a trust relationship, a person will listen to the opinions from others when he wants to make a decision. In Grid computing, when the entities want to make a trust-based decision, the entities may also rely on others for the information and opinion pertaining to a specific entity. For example, if entity x wants to make a decision of whether to call the service s1 of domain y, which is unknown to x, then x can rely on the reputation of the service s1 of domain y. In this paper, we adopt the definition of Reputation as presented in [3] with modification:

> *The reputation of an entity is an expectation of its behavior based on its identity and other entities' observations or information about the entity's past behavior within a specific context at a given time.*

Please note that our trust and reputation definition are both associated with the identity trust and behavior trust while in [3], only behavior trust is concerned.

3 Context in Grid Computing Systems

In the previous section, we mentioned that trust is defined to be context specific. Thus, what is context with respect to a Grid computing system? A service invocation scenario is illustrated in Figure 1.

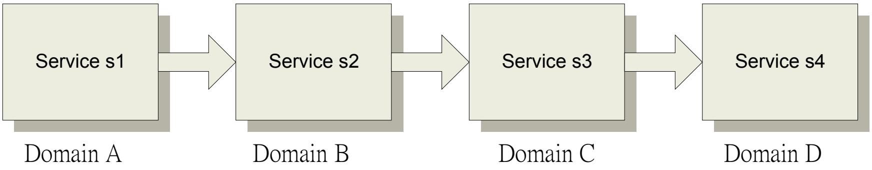

Fig. 1. Service Invocation

In Figure 1, service instance s1 invokes service instance s2, service instance s2 further invokes service instance s3 and then service instance s3 calls service instance s4 finally. In this scenario, we define the Grid context as an ordered four-tuple (id_{s1},id_{s2},id_{s3},id_{s4}) where $id_{service}$ is a globally unique service instance id of a particular service.

Therefore, to define context in a Grid computing system, if the service invocation is originated from service s_1,s_2 .... up to s_n, the context will be an ordered n-tuple (ids_1,ids_2,......,ids_n).

4 Trust Tree

The context of the Grid is service-based. The advantage of the service-based context is that it is highly precise to identity a particular service invocation. However, as there may be many different service instances in a domain, service-based context implies that the number of different contexts can be huge. In a trust system, different contexts should have different trust values. Thus, if we store the trust values in a table and search for the trust value sequentially, it will take quite a long time to do so.

To be efficient, instead of using a simple table to store the direct trust value or reputation from other domains, we propose a trust tree structure. The trust values will be stored in a structure called a trust tree. For each trust value, the associated context tuple will be regarded as a n-dimension record and becomes a node of our trust tree. Other context-based information will become annotations for that node. A trust tree is shown in Figure 2 for illustration.

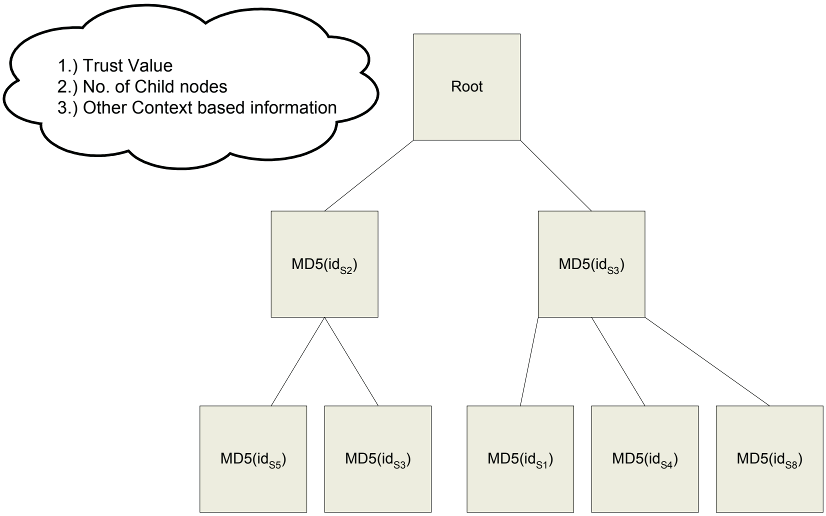

Fig. 2. A sample trust tree

The following statements summarize the structure of a trust tree:

1) Each node of our tree contains the MD5 digest of the corresponding service instance id (128-bit) as the key.
2) Each node may consists of zero to n children nodes.
3) To retrieve a child node efficiently, all the children nodes will be sorted according to the key value and the number of children nodes will be stored in the parent node such that when a key value is given, a binary search could be performed so as to find the matching child node.

Besides, the trust tree provides a *similarity* operation that enables us to search out the trust value of a similar-context node. Consider if we are now making a trust evaluation towards a service request, using the trust tree, we can refer to some similar-context service requests. Undoubtedly, these similar-context service requests do provide a good source for evaluating the trust value of the current service request and leads to a better trust evaluation.

5 Conclusion

In this paper, to integrate "trust" in the Grid Computing Systems, we suggest to address both identity trust and behavior trust. Besides, we give the definition of context in Grid Computing and it makes the meaning of trust to become much more precise and clear. On the other hand, to manage the trust values in an efficient way, we define a trust tree structure. The Trust tree also provides a *similarity* operation that enables us to find out the trust value of other transactions with similar context. It is definitely useful for trust evaluation.

References

1. Alfarez Abdul-Rahman, Stephen Hailes, "Supporting Trust in Virtual Communities," In: Proceedings Hawaii International Conference on System Sciences 33, Maui, Hawaii, 4-7 January 2000.
2. I. Foster et al., "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration," Argonne National Laboratory, Argonne, Ill. (2002)
3. Farag Azzedin and Muthucumaru Maheswaran, "Evolving and Managing Trust in Grid Computing Systems," Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering
4. Geoff Stoker, Brian S. White, Ellen Stackpole, T.J. Highley, and Marty H, Toward Realizable Restricted Delegation in Computational Grids, HPCN Europe 2001, LNCS 2110, pp.32-41, 2001.
5. Ian Foster, Carl Kesselman, and Steve Tuecke, The Anatomy of the Grid, Enabling Scalable Virtual Organizations, International Journal of Supercomputer Applications, 2001.
6. Ian Foster, The Grid: A New Infrastructure for 21st Century Science, Physics Today, February 2002.