https://doi.org/10.26552/com.C.2016.3.41-49

Slavomir Kavecky - Penka Martincova*

AD HOC GRID RESOURCE MANAGEMENT: GRID SECURITY

The purpose of security in ad hoc grid environments is to support secure execution of tasks on shared resources and to protect the resources from malicious user actions. The concept of trust management is capable to solve the security issues by incorporating trust into the process of decision making. The quality of the decisions is dependent on a correct assessment and representation of trustworthiness assigned to the potentially collaborating parties. In most cases the value of trustworthiness is derived at least from direct trust and recommendations, but other factors as risk, uncertainty, context dependent information and attributes characterizing the task and the shared resource should be included in the derived value as well. This paper presents a specification of parameters relevant for an accurate trust evaluation.

Keywords: *Ad hoc grid, trust management, trust aware grid security, trust aware job scheduling.*

1. Introduction

Generally, the grid security protects shared resources against malicious actions of users and other entities that could damage the resources or corrupt the integrity of data stored and processed on the resources. However, in many situations the users of the ad hoc grid have to be protected from those who offer the resources, so the issue is also vice-versa [1].

Authentication and authorization, which are referred to as hard security mechanisms, do not allow any occurrence of risk or uncertainty (the user is either authenticated and authorized to access a shared resource or is not), but collaborations in an open environment are necessarily coupled with potential dangers that necessitate reasoning about risk and uncertainty. Trust was recognized as an important aspect of decision making in many distributed systems and it is used as a mechanism for managing dangers and learning from past interactions in order to reduce the risk exposure. For example, trust and reputation systems support decision making on the Internet provided services, which are based on a trust derived from ratings assigned to a certain provider by customers after completion of a transaction. Other parties can use the trust and reputation derived from the aggregated ratings to decide whether or not to run a transaction with the rated party in the future. Trust management, which is referred to as a soft security, represents the shift from attempting to provide absolute protection against potential dangers to accepting dangers as an intrinsic part of any global computing [1 and 2].

The aim of the paper is to present a detailed classification and specification of parameters that can be used for an accurate evaluation of trustworthiness assigned to a grid entity. The reminder of the paper is organized as follows: Section 2 presents a short overview of trust models integrating trust management into ad hoc grid computing; Section 3 describes the process of job scheduling performed in ad hoc grid environment; Section 4 provides classification of parameters needed for trust evaluation, describes relations between the parameters and proposes a procedure inferring the parameters into a final trust value; The verification of the proposed trust management integration into the ad hoc grid infrastructure is described in section 5; and finally, the section 6 concludes the paper.

2. Related work

The incorporation of trust management into the grid infrastructure has been a subject of research for several years. Model proposed by Azzedin and Maheswaran [3] is one of the first models introducing trust management as a part of the grid computing. In the model authors classify trust into two categories: identity trust and behavior trust. However, the evaluation and update of trust is derived only from the behavior trust, which is concerned with observations of past collaborations. The identity trust dealing with verification of entity's identity and determination of assigned authorization permissions is left out. The model also omits the integration of risk and uncertainty into the trust value, but as already stated there is no need for reasoning about trust if risk and uncertainty are not involved. The main asset of the model is the introduction of trust between

* **Slavomir Kavecky, Penka Martincova**
Faculty of Management Science and Informatics, University of Zilina, Slovakia
E-mail: slavomir.kavecky@fri.uniza.sk

two collaborating entities as a bidirectional relationship, where the trust of one entity in other entity differs from the trust of the other entity in the first entity. Therefore, the collaboration among entities is not executed unless both parties see each other as trustworthy.

The trustworthiness of a resource entity in the model proposed by Song et al. [4 and 5] is dependent on its self defense capability and reputation determined from prior collaborations and is referred to as a trust index. On the other hand, the user demands minimal required security assurance, which may appear as a request for authentication, data encryption, access control, etc., and is referred to as a security demand. During the process of assigning jobs onto resources the condition *Security Demad* ≤ *Trust Index* must be satisfied in order to start the jobs on the selected resources. The trust index assigned to the resource corresponds to a wider notion of trustworthiness and is derived from behavior trust as well as from the attributes of the resource. Risk and uncertainty are still omitted and are not part of the final trust index value. The main drawback of this model is evaluation of trustworthiness from only the user's point of view. The resource has no means to determine the trustworthiness of the user and to make trust based decision on whether or not to collaborate with the user.

Explicit usage of uncertainty as a part of trust value is presented in the model proposed by Lin et al. [6]. Trust is evaluated as a combination of belief and disbelief in the entity's trustworthiness and uncertainty as a filling of the absence of both belief and disbelief. The value of trust is deduced from the user's and also from the resource provider's point of view. The model also states that the user and the resource provider are interested in different types of trust. The user is interested in execution trust, which represents the ability of the provider to faithfully allocate appropriate resources to enable successful completion of the job. From the provider's point of view trust in the user is defined as a belief in the ability of the user to produce competent user code and it is referred to as code trust.

The model proposed by Shi et al. [7] introduces several novelties previously not considered in the trust models. Trust of one entity in another entity (in the model determined as a combination of direct experiences and experiences of other subjects) is influenced by a particular situation, in which the collaboration is about to take place, and is referred to as a situational trust. Different situations require different considerations with regard to trust and result in different values of trust. In case two entities have just encountered, the model introduces the initial trust as means to represent the basic trusting disposition of unknown entity and is derived from all previous experiences in all situations through the entire life time of the trusting entity. Despite the novelties the model is introducing, it has a few drawbacks. It lacks integration of risk into the trust value and uncertainty is expressed only indirectly through initial trust evaluated in case full information about trusted entity is missing.

Over the last decade more models emerged that express trust value as a combination of behavioral trust corresponding to the observations of past collaborations and trust derived from attributes describing the current state of evaluated entity. A more detailed overview of these models is presented in our previous work [8].

3. Trust Aware Ad Hoc Grid Scheduling

The purpose of the trust management in the ad hoc grid environment is to guarantee the quality of services provided by the grid nodes and the quality of user's behavior. The integration of trust into the ad hoc grid infrastructure is coupled inseparably with the scheduling of jobs on the provided resources. However, there are some differences between the ad hoc and the traditional grid scheduling when the trust management is involved.

In order to integrate trust management into the ad hoc scheduling process, the steps executed during the resource discovery, system selection and job execution must perform the following additional tasks: *(i)* definition of minimal trustworthiness needed to begin the collaboration between the user and the resource provider*, (ii)* determining the current trustworthiness of the involved nodes, *(iii)* and update of trustworthiness after the job completion.

It is evident that these tasks impose new requirements on the ad hoc grid architecture. The architecture depicted in Fig. 1 introduces the trust manager module as a solution to meet the imposed requirements.

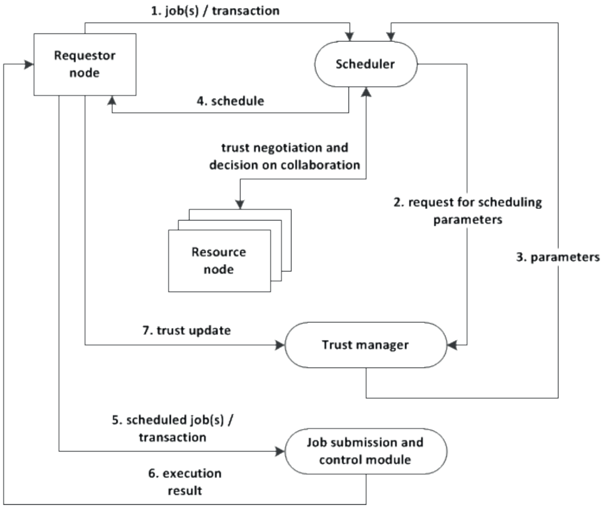

1. job(s) / transaction
Requestor node
Scheduler
4. schedule
trust negotiation and decision on collaboration
2. request for scheduling parameters
Resource node
3. parameters
7. trust update
Trust manager
5. scheduled job(s) / transaction
Job submission and control module
6. execution result

Fig. 1 Trust manager integration into the ad hoc grid infrastructure from the requester's point of view

During the phase of resource selection the user defines the job and the requirements needed for the job to run. To select a trustworthy resource, the user defines the security demand [4 and 5], which is taken as a constraint during the system selection step. The security demand is determined either directly by the user as one of the job requirements, or by the trust manager according to the parameters provided by the user.

The resources that passed the authorization and minimal filtering requirements are assigned a trust index [4 and 5] determined by the trust manager on the basis of static and dynamic information about the resources, job definition parameters and other factors managed by the trust manager. The trust index is a combination of more parameters, but which parameters and how exactly they are used for the trust index evaluation depends on the used trust model. The minimal components of the calculated value are the direct trust and the recommendations. However, other factors as risk, uncertainty and context dependent information should be included in the trust index as well. It is important to note that the scheduler uses the security demand and the trust indexes obtained from the trust manager only to exclude the untrustworthy resources. The schedule optimization itself is not affected and still corresponds only to the quality of services demanded by the user.

The resource provider demands a certain level of trustworthiness as well as the user. Therefore, after the exclusion of untrustworthy resources the scheduler requests the most optimal and trusted resource to consent to the future collaboration. The decision whether or not to accept the collaboration is based on the resource's security demand and the trust index assigned to the requesting node. Both values are obtained from the resource's trust manager on basis of job parameters included in the request, recommendations, previous experiences, uncertainty, risk and other factors. The decision on the collaboration is responded back to the scheduler. In case of negative response the scheduler sends the request for consent to the next most optimal resource until an affirmative answer is received.

The job scheduled with the help of the trust manager is forwarded to a module responsible for job submission and execution. After the job completion the result of the execution is transferred to the requester node. The trust update is the final step involving the trust manager module on the requester node as well as the resource node. The update is performed according to a positive or a negative experience resulting from the job execution and is necessary for correct representation of trust in the collaborating parties.

4. Trust Aware Ad Hoc Grid Security

The collaborations in the grid environment are executed by two types of entities: user and resource provider. User and resource provider require protection against malicious behavior that can take form of user's program containing malicious code capable to compromise the provider's resource node or it can take a form of a malicious resource node capable to harm the user's job running on the provided resource.

The security infrastructure incorporating trust should be based on a trust model that is capable to support or enhance the functional aspects of the grid infrastructure. The model should be also capable to process evidence of the previous collaborations and to transform it together with other relevant parameters into a trust value that is part of the security decisions for both the user and the resource provider protection.

4.1 Parameters Classification

Each participant of collaboration in the grid environment has his own set of expectations for the quality and performance of the collaboration and is satisfied with the executed collaboration only if the required expectations are met. Trust in this context can be used to express the confidence of the relying entity that a collaborating party will meet the desired expectations. The expectations for the quality of collaboration placed by the users and resource providers are mapped to system parameters and capabilities that can be abstracted into three groups of trust component: *(i)* behavioral parameters, *(ii)* system attributes *(iii)* and descriptive attributes.

Behavioral parameters (e.g. accessibility, availability, competence and reliability) describe the behavior of collaborating entities and are used to create history of data obtained from past interactions. By analyzing the history of the collected data using statistical methods together with the entity's personalized notion of normal or anomalous behavior it is possible to predict the outcome of future collaborations.

System parameters (e.g. authentication and authorization mechanism, utilized security mechanisms, maintenance of data integrity, etc.) describe the technical parameters and capabilities of the provider's shared resources and the user's node serving as access point into the grid community. The system attributes are characterized by a slow change over time. Over a period of time the attribute values do not change gradually, but the change is made suddenly and is noticeably large.

In contrast with behavioral and system attributes the **descriptive parameters** (e.g. benefit and loss associated with a particular collaboration, amount of observed behavioral parameters, time passed since last collaboration, etc.) do not describe the trusting disposition of the relying entity in the collaborating party, but they indicate the level of security assurance required by the relying entity. In a particular collaboration context the security assurance corresponds to the minimal trustworthiness of the collaborating party required by the relying entity.

4.2 Determining Trust from Parameters

The incorporation of trust management into the grid infrastructure should support the fundamental functional aspects of the grid as resource allocation and execution of tasks. The scheduling of tasks is responsible for finding an appropriate resource node meeting the required security assurance expressed as a security demand. Similarly, the resource node declares its own security demand that must be fulfilled by the user in order to process his request by the resource node.

The **security demand** is dependent on the risk and uncertainty (as depicted in Fig. 2) perceived by the relying party in the context of a particular collaboration. In a risky situation the relying party requires a high level of security assurance provided by the collaborating party in order to start a collaboration. Of course, the required security assurance is lower in case of a less risky situation. The uncertainty influences the security assurance in a similar manner. The higher the level of uncertainty the less certain about a collaboration execution the relying party becomes. Therefore, the required level of security assurance increases as well.

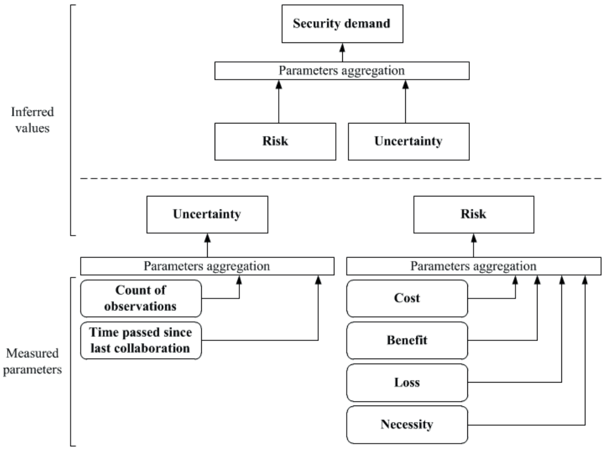


Fig. 2 Security demand inferred from trust components

The more important a flawless collaboration the more severe the damage will become in case of failure. The likelihood of failure occurrence and the cost incurred to the relying party is referred to as the **risk**. Risk and trust are related in the sense that there is no need for a trusting decision unless there is a risk involved. The measurable parameters used for inferring the value of risk as depicted in Fig. 2 are [1, 9 and 10]: *(i)* cost of collaboration, *(ii)* benefit *(iii)* loss, *(iv)* and necessity of a collaboration execution.

Uncertainty refers to a situation where the relying party cannot be fully sure about the accuracy of the decision. For example, a situation can occur where two completely unknown entities have to collaborate, but they have neither the experiences with each other, nor recommendations from other entities are available. A similar situation can also occur if only a part of the information is available and other decision factors are missing. The measurable parameters used for inferring the value of uncertainty as depicted in Fig. 2 are: *(i)* count of observations *(ii)* and time passed since the last collaboration.

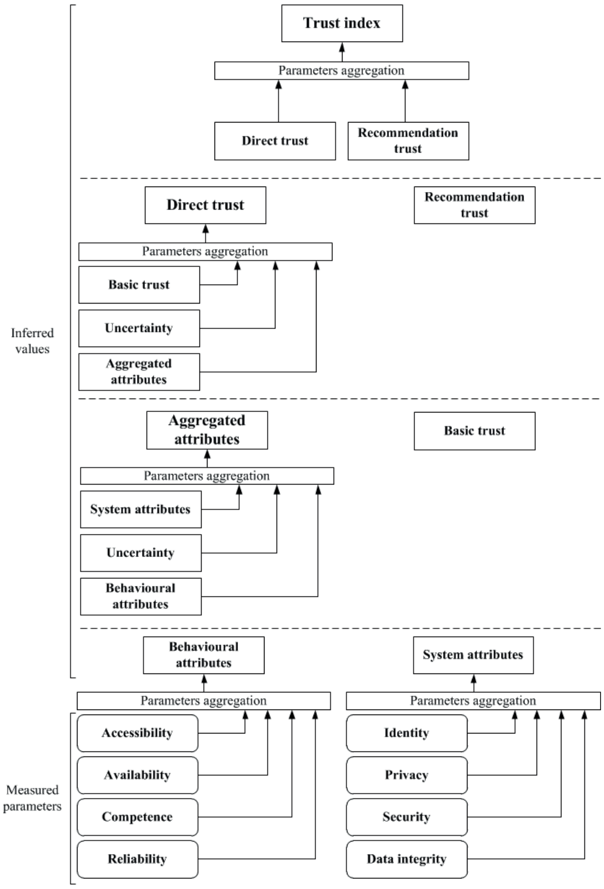


Fig. 3 Trust index inferred from trust components

Trust index, which specifies the trustworthiness of a collaborating party, is dependent on direct trust and recommendations (as depicted in Fig. 3). Recommendations are obtained from other entities of the grid environment and correspond to the reputation of the recommended entity. Reputation can be described as everything that is generally said or believed about the entity's character or standing. If the relying party is aware of the collaborating entity's reputation it can base its trust on that reputation, i.e. the collaborating entity is trusted because of its good reputation. Similarly, the entity becomes distrusted in case of its bad reputation.

Direct trust represents the private knowledge the relying party has about the collaborating entity and is formed from previous interactions, current context of the collaboration and attributes characterizing the collaborating entity. The direct trust and recommendations have different effect on the inferred trust index. The private knowledge of the relying entity in form of direct trust is capable to overrule the reputation of the collaborating entity, i.e. in case of high direct trust the collaborating entity is trusted despite its bad reputation and similarly, in case of low direct trust the entity is distrusted despite its good reputation. The capability of the direct trust to overrule the recommendations is dependent on the weights assigned to these two parameters. As depicted in Fig. 3, the parameters used for inferring direct trust are: *(i)* basic trust, *(ii)* aggregated attributes, *(iii)* and uncertainty.

The **aggregated attributes** (as depicted in Fig. 3) are inferred from system and behavioral attributes. Uncertainty represents a weighting factor determining the relative importance of the considered attributes. The impact of system attributes is higher than the impact of behavioral attributes in case of high uncertainty and the behavioral attributes affect the inferred value more significantly in case of low uncertainty. Exact value of aggregated attributes can be inferred from the following system attributes (as depicted in Fig. 3): *(i)* identity, *(ii)* privacy, *(iii)* security, *(iv)* and data integrity. According to the models dealing with behavior trust [11, 12 and 13] the behavior of entity can be described with the following attributes (as depicted in Fig. 3): *(i)* accessibility, *(ii)* availability, *(iii)* competence, *(iv)* and reliability.

5. Experimental Results

The verification of the proposed model for trust value calculation and the trust management integration was carried out by a computer simulation. The simulation was performed using the GridSim simulation toolkit [14]. The verification of the modeled ad hoc grid infrastructure is evaluated according to the metrics specified in the section 5.3. The verification consists of two experiments. The first experiment was performed without the trust management integration and provides reference values describing the capabilities of the modeled ad hoc grid infrastructure. The latter experiment was performed with the trust management integration and shows the effect of the proposed trust value calculation and trust management integration on the secure execution of collaborations.

The model of the ad hoc grid infrastructure executed by the simulation toolkit consists of ten user entities and ten resource provider entities. The modeled entities were assigned several system capabilities and forms of behavior (Table 1, 2, 3 and 4). The capabilities and forms of behavior assigned to the modeled entities were used for trust calculation according to the model described in the section 4. Security demand and trust index, which are used for decisions making whether or not to start a collaboration, are values inferred from various system attributes, parameters describing the behavior of collaboration participant and context dependant parameters. As depicted in the Figs. 2 and 3, only the parameters used for inferring behavioral attributes, system attributes, risk and uncertainty are obtained as the result of measurement. All other parameter values are inferred from parameters placed one level below (except recommendations and basic trust, which values are obtained in a separate manner).

Each of the measurable parameters is measured directly or can be broken up in measurable elements. The parameters used for inferring the value describing the behavior of grid entity are measured directly according the entity's behavior elements observed over multiple collaborations. Considering the collaboration participant *X* as trustor and *Y* as trustee, the calculated value of inferred behavioral attributes V_x is based on the entirety of *N* behavior elements under observation and is expressed according to the following formula:

$$V_x = \frac{\Sigma_{i=1}^{N} E(Y)_i}{N} \qquad \text{Formula 1}$$

where $E(Y)_i$ represents value assigned to the *i*-th behaviour element under observation. Each observed element is calculated as the number of "positive" observations (the good behavior was observed) divided by the total number of observations, as generalized in the formula 2:

$$E(Y)_i = \frac{\text{"positive" observations of the } i - th \text{ element}}{\text{all observations of the } i - th \text{ element}} \qquad \text{Formula 2}$$

The parameters used for inferring the value describing the system properties of grid entity either are evaluated directly, or they are broken up in measurable and evaluable elements. Considering the collaboration participant *X* as trustor and *Y* as trustee, the value of inferred system attributes V_x is based on the entirety of *N* measured system parameters and is expressed according to formula 1 where $E(Y)_i$ represents value assigned to the *i*-th evaluated system parameter. The value of identity and privacy parameters is calculated as the value assigned to measurable element associated with the system parameter divided by the maximal attainable value as generalized in formula 3:

$$E(Y)_i = \frac{\text{value assigned to the } i - th \text{ measurable element}}{\text{maximal attainable value of the } i - th \text{ element}} \qquad \text{Formula 3}$$

In case of security and data integrity parameters, the value $E(Y)_i$ is calculated as the sum of *n* values assigned to the measurable element associated with the system parameter divided by the maximal value attainable by the measurable element as generalized in formula 4:

$$E(Y)_i = \frac{\Sigma_{j=1}^{n} j - th \text{ value assigned to the } i - th \text{ measurable element}}{\text{maximal attainable value of the } i - th \text{ element}} \qquad \text{Formula 4}$$

A more detailed measurement and evaluation procedure of modeled behavioral attributes and system parameters is presented in our previous work [15].

Characteristics of the users (1 - 5) modeled in the computer simulation Table 1

Characteristic	**User**				
	1	2	3	4	5
Antivirus protection	Yes	Yes	Yes	Yes	Yes
Firewall	Yes	Yes	Yes	Yes	Yes
Intrusion detection system	No	No	No	No	No
Transport layer security	Yes	Yes	Yes	Yes	Yes
IPsec	No	No	No	No	No
Rate of faulty tasks	No faulty tasks	Very low occurrence rate	Low occurrence rate	Low occurrence rate	Common occurrence rate

Characteristics of the users (6 - 10) modeled in the computer simulation Table 2

Characteristic	User				
	6	7	8	9	10
Antivirus protection	Yes	Yes	Yes	Yes	Yes
Firewall	Yes	Yes	Yes	Yes	Yes
Intrusion detection system	No	No	No	No	No
Transport layer security	Yes	Yes	Yes	Yes	Yes
IPsec	No	No	No	No	No
Rate of faulty tasks	Common occurrence rate	High occurrence rate	High occurrence rate	Very high occurrence rate	Very high occurrence rate

Characteristics of the resource provider nodes (1 - 5) modeled in the computer simulation Table 3

Characteristic	**Resource provider**				
	1	2	3	4	5
Antivirus protection	Yes	Yes	Yes	Yes	Yes
Firewall	Yes	Yes	Yes	Yes	Yes
Intrusion detection system	No	No	No	No	No
Transport layer security	Yes	Yes	Yes	Yes	Yes
IPsec	No	No	No	No	No
Sandbox	No	No	No	No	No
Authentication type	X509 certificate	X509 certificate	X509 certificate	X509 certificate	X509 certificate
Authorization type	Role based authorization	Role based authorization	Role based authorization	Role based authorization	Role based authorization
MIPS	2700	2350	2000	2350	2350
Rate of resource non-availability	Always available	Always available	Always available	Very low occurrence rate	Low occurrence rate
Rate of task execution failure	No failures	No failures	No failures	Common occurrence rate	Common occurrence rate

Characteristics of the resource provider nodes (6 - 10) modeled in the computer simulation Table 4

Characteristic	Resource provider				
	6	7	8	9	10
Antivirus protection	Yes	Yes	Yes	Yes	Yes
Firewall	Yes	Yes	Yes	Yes	Yes
Intrusion detection system	No	No	No	No	No
Transport layer security	Yes	Yes	Yes	Yes	Yes
IPsec	No	No	No	No	No
Sandbox	No	No	No	No	No
Authentication type	X509 certificate	X509 certificate	X509 certificate	X509 certificate	X509 certificate
Authorization type	Role based authorization	Role based authorization	Role based authorization	Role based authorization	Role based authorization
MIPS	2350	2700	2000	2700	2000
Rate of resource non-availability	Common occurrence rate	High occurrence rate	High occurrence rate	Very high occurrence rate	Very high occurrence rate
Rate of task execution failure	Common occurrence rate	High occurrence rate	High occurrence rate	Very high occurrence rate	Very high occurrence rate

5.1 Experiment 1 – Ad Hoc Grid without Trust Management

The first experiment was carried out by the simulation toolkit according to the modeled ad hoc grid infrastructure without incorporation of the trust management. The values measured during the simulation represent reference values describing the capabilities and qualities of the modeled infrastructure. The values were used for comparison to values measured during other experiments.

Count of tasks executed without trust management integration into the modeled ad hoc grid infrastructure Table 5

Task type	Measured values	
		Percentage of the executed tasks [in %]
All executed tasks	5833.10	100.00
Successful tasks	4880.36	83.67
Failed tasks	952.74	16.33

During the experiment 1000 simulation runs were executed. The count of all tasks, successful tasks and failed tasks are given as an arithmetic mean calculated from the values measured in each simulation run. Table 5 shows the count of all tasks executed during the first experiment, as well as the count of successful and failed tasks. The table also shows the percentage of the executed tasks. The count of all tasks is 5833.10, count of successful tasks is 4880.36 (83.67% of all executed tasks) and count of failed tasks is 952.74 (16.33% of all executed tasks).

5.2 Experiment 2 – Ad Hoc Grid with Trust Management

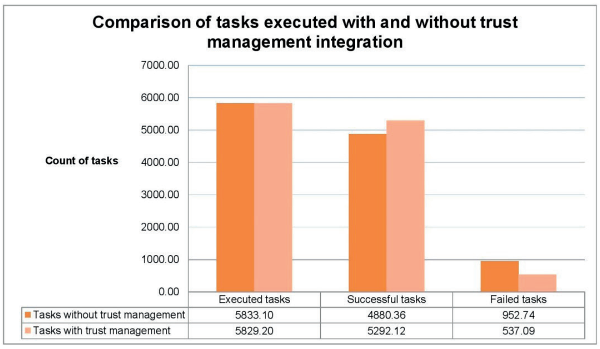
During the experiment 1000 simulation runs were executed. The count of all tasks, successful tasks and failed tasks are given as an arithmetic mean calculated from the values measured in each simulation run. The second experiment was carried out by the simulation toolkit according to the modeled ad hoc grid infrastructure with the incorporation of trust management. Table 6 shows the count of all tasks executed during the second experiment, as well as the count of successful and failed tasks. The table also shows the percentage of the executed tasks. The count of all tasks is 5829.20, count of successful tasks is 5292.12 (90.79% of all executed tasks) and count of failed tasks is 537.09 (9.21% of all executed tasks).

Count of tasks executed with trust management integration into the modeled ad hoc grid infrastructure Table 6

Task type	Measured values	
		Percentage of the executed tasks [in %]
All executed tasks	5829.20	100.00
Successful tasks	5292.12	90.79
Failed tasks	537.09	9.21

5.3 Evaluation Results

The verification of the modeled ad hoc grid infrastructure is evaluated according to the following quantitative metrics: *(i)* competence *(ii)* and reliability. The competence corresponds to the capability of the modeled ad hoc grid infrastructure to support execution of user tasks. The competence is measured as count of all tasks executed during the simulation. The reliability corresponds to the capability of the modeled ad hoc grid infrastructure to support secure execution of user tasks. The reliability is measured as count of failed tasks observed during the simulation.



	Executed tasks	Successful tasks	Failed tasks
■ Tasks without trust management	5833.10	4880.36	952.74
■ Tasks with trust management	5829.20	5292.12	537.09

Fig. 4 Comparison of tasks executed with and without trust management integration into the modeled ad hoc grid infrastructure.

Figure 4 shows that there is almost no difference in the count of all tasks executed during the first and second experiment. The integration of trust management into the ad hoc grid infrastructure has no negative effects on the infrastructure competence to execute user tasks. On the other hand, the integration of trust into the ad hoc grid infrastructure affects the capability of the infrastructure to support secure execution of user tasks in a considerable manner. Figure 4 shows that the proposed incorporation of trust management results in reduced count of failed tasks and improves the reliability of the ad hoc grid infrastructure. The percentage of improvement in the modeled ad hoc grid reliability is equal to 43.62%. This proves the capability of the proposed trust model to ensure the secure execution of collaborations mediated through the ad hoc grid infrastructures.

6. Conclusion

The paper presents an ad hoc grid architecture integrating trust manager module taking over tasks as trustworthiness assessment of collaborating nodes and update of trustworthiness after a job completion. The procedure of trust evaluation is a complex process including procession of various trust components and relations among these components. The paper describes in detail these relations and their impact on the inferred values produced by the trust management inference system. The values are deduced from parameters describing the most significant system attributes and behavioral traits of evaluated grid entities. The verification of the proposed trust management integration into the ad hoc grid infrastructure was carried out by a computer simulation proving the capability of the proposed trust management integration to execute collaborations in a more secure manner.

References

[1] JOSANG, A., KESER, C., DIMITRAKOS, T.: Can We Manage Trust? *Trust Management*, vol. 3477 of Lecture Notes in Computer Science, pp. 93-107, Springer: Berlin : Heidelberg, 2005.

[2] JOSANG, A., ISMAIL, R., BOYD, C.: A Survey of Trust and Reputation Systems for Online Service Provision, *Decision Support Systems*, 43(2), 618-644, 2007.

[3] AZZEDIN, F., MAHESWARAN, M.: Evolving and Managing Trust in Grid Computing Systems, Canadian Conference on Electrical and Computer Engineering, 2002, pp. 1424-1429, 2002.

[4] SONG, S., HWANG, K., KWOK, Y. K.: Trusted Grid Computing with Security Binding and Trust Integration. *J. of Grid Computing*, 3(1-2), 53-73, 2005.

[5] SONG, S., HWANG, K., MACWAN, M.: Fuzzy Trust Integration for Security Enforcement in Grid Computing. *Network and Parallel Computing*, vol. 3222 of Lecture Notes in Computer Science, pp. 9-21. Springer: Berlin : Heidelberg, 2004.

[6] LIN, CH., VARADHARAJAN, V., WANG, Y., PRUTHI, V.: Enhancing Grid Security with Trust Management, Proceedings of the 2004th IEEE International Conference on Services Computing, 2004, pp. 303-310, 2004.

[7] SHI, J., BOCHMANN, G., ADAMS, C. A.: Trust Model with Statistical Foundation, IFIP International Federation for Information Processing: Formal Aspects in Security and Trust, pp. 145-158, 2005.

[8] KAVECKY, S., MARTINCOVÁ, P.: Overview of Trust Models Integrating Trust Management into Grid Computing, *International Journal of Computer Applications*, 129(7), pp. 1-6, 2015.

[9] JOSANG A., PRESTI, S. L.: Analysing the Relationship between Risk and Trust. *Trust Management*, vol. 2995 of Lecture Notes in Computer Science, pp. 135-145, Springer: Berlin: Heidelberg, 2004.

[10] ENGLISH, C., TERZIS, S., WAGEALLA, W.: Engineering Trust Based Collaborations in a Global Computing Environment. *Trust Management*, vol. 2995 of Lecture Notes in Computer Science, pp. 120-134, 2004.

[11] DIONYSIOU I., GJERMUNDROD, H., GUTS, S: *Simplified Grid user Trust Service for Site Selection.* The 7th Intern. Conference on Internet Monitoring and Protection, 2012, pp. 40-46, 2012.

[12] MANUEL, P., THAMARAI SELVI, S., BARR, M. E.: Trust Management System for Grid and Cloud Resources. 1st Intern. Conference on Advanced Computing, 2009, pp. 176-181, 2009.

[13] PAPALILO E., FREISLEBEN, B.: Managing behaviour Trust in Grid Computing Environments. *J. of Information Assurance and Security*, 3, 27-37, 2008.

[14] BUYYA R., SULISTIO, A.: *Service and Utility Oriented Distributed Computing Systems: Challenges and Opportunities for Modeling and Simulation Communities.* Simulation Symposium, ANSS 2008, 41st Annual, pp. 68-81, April 2008.

[15] KAVECKY, S., MARTINCOVA, P.: Specification of Parameters Relevant for Trust Evaluation in an Adhoc Grid Environment, *Intern. J. of Computer Applications*, 132(11), pp. 1-8, 2015.