# Ad Hoc Grid Resource Management: Grid Security

Slavomír Kavecký*
Faculty of Management Science and Informatics
University of Žilina
Univerzitná 8215/1, 010 26 Žilina, Slovakia
slavomir.kavecky@fri.uniza.sk

## Abstract

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 mechanisms of authentication and authorization commonly used in traditional grid environments are not sufficient to cover all security requirements arising from the decentralized nature of the ad hoc grid. The concept of trust management is capable to solve the security issues by incorporating trust into the process of decision making. The quality of made 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 dependant information and attributes characterizing the task and the shared resource should be included in the derived value as well. This paper presents an overview of the trust evaluation process and provides a specification of parameters relevant for an accurate trust evaluation.

## Categories and Subject Descriptors

C.1.4 [**Parallel Architectures**]: Distributed architectures—*traditional grid infrastructure, ad hoc grid infrastructure*; K.6.4 [**System Management**]: Centralization/ decentralization—*job scheduling*; D.2.0 [**General**]: Protection mechanisms—*trust aware grid security and job scheduling*

## Keywords

Traditional grid, ad hoc grid, trust management, trust aware grid security, trust aware job scheduling

## 1. Introduction

Recently, large data processing and high-performance computing has become more available for the public. Grid[9], which is one of the leading technologies enabling these capabilities, is characterized by heterogeneity and geographical dispersion of its nodes serving as resources for job execution or as access points into the grid environment. According to the OGSA (Open Grid Services Architecture)[10] the following capabilities should be typical for any grid middleware: user tasks execution management, data manipulation management, shared resources allocation and management, secure job execution and resource sharing, information provision of executed tasks and shared resources, and finally support for the grid configuration.

As stated above, job scheduling and secure execution of jobs are core services enabling provision of the main grid capabilities – sharing and utilization of available dispersed resources. The traditional grid infrastructures (the most known traditional grid infrastructures are Globus Toolkit [13], Gridbus Middleware [12] and UNICORE [25]) implement scheduling and security in accordance to their centralized nature. In the ad hoc grids (the most known ad hoc grid infrastructures are OurGrid [3, 24] and MoGrid [11]), which are well known for structural independence and decentralized architecture, scheduling and security are managed by participating nodes without depending on any external infrastructure for assistance.

The aim of the paper is to present a brief description of trust management and trust evaluation, as well as 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 provides a brief introduction to the trust management and trust evaluation; Section 3 surveys the state of the art in traditional and ad hoc grid security provision; Section 4 describes the process of job scheduling performed in ad hoc grid environment; Section 5 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 6; Section 7 describes the future work in the field; and finally, section 8 concludes the paper.

## 2. Trust and Trust Management

The notion of trust is used with variety of meanings and without any unified definition. However, in the literature are used two common definitions with well understood distinction between them. The **reliability trust** [15, 16] is defined as follows: *Trust is a subjective probability by*

*Recommended by thesis supervisor: doc. Ing. Penka Martincová, PhD.
Defended at Faculty of Management Science and Informatics, University of Žilina in Žilina on XX XX, 2016.

*which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.* The **decision trust** [15, 16] is defined as follows: *Trust is an extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.*

The reliability trust enables to make decisions whether or not to start a collaboration only on the basis of the collaborator's reliability estimation. On the other hand, the decision trust defines context as a part of the trust value and binds the estimation of the collaborator's reliability with a risk that arises from the uncertain outcome of the collaboration. Therefore, the decision trust seems to be a better choice for the purpose of trust modelling.

Trust between two entities is a bidirectional relationship and can be seen from multiple points of view. Humans tend to collaborate only with trusted individuals. Generally speaking, the success and survival of an entity is dependent on the willingness of other entities to collaborate. There are many genetically determined or culturally acquired strategies helping the people to appear reliable and trustworthy. The easiest and probably most used strategy for gaining trust is simply to behave in a trustworthy and reliable manner. However, the attempt to give a false impression of trustworthiness for the purpose of a personal gain is not uncommon. Therefore, it is important not only to represent own trustworthiness, but also determine correctly the trustworthiness of the target entities.

**Trust management** [16] is defined as follows: *The activity of creating systems and methods that allow relying parties to make assessments and decisions regarding the dependability of potential transactions involving risk, and that also allow the players and system administrators to increase and correctly represent the reliability of themselves and their systems.*

The parties in a computer mediated communication and collaboration need methodologies enabling them to assess properly the trustworthiness of remote parties, as well as to be recognized as trustworthy by the remote parties. This need arises due to the fact that the computer networks move the collaboration participants away from a direct style of interaction. They can collaborate with people they have never met and that they might never meet in person. Therefore, the traditional methods of trustworthiness assessment and representation used in a physical world can no longer be used. Simply expressed, the application of methodologies that enable such trusted collaborations in online environments can be called trust management [16].

Trust is a directional relationship between a trustor and a trustee, whereby the trustor is a thinking entity making decisions whether or not to start collaboration with the trustee on the basis of the trustee's trustworthiness. In a grid the trust between the grid user and the resource provider is a mutual bidirectional relationship, because the user and the provider must be trustworthy to each other, otherwise the collaboration is not possible.

The mutual trust relationship can be described by the trust classes[15] as follows:

- **Provision trust** describes the user's trust in a service or in a resource provider. The user trusts the provider to provide services that implement the advertised functionality and do not harm the user's resources. The provision trust ensures the reliability of the provider and is related to the integrity of the user's data stored in and/or obtained from the provided resources.
- **Access trust** describes the provider's trust in the user intending to access to the offered resource, i.e. the provider trusts the user to use the resource in an agreed manner. This relates to the access control paradigm which is a central element in a computer security.
- **Delegation trust** describes the trust in an agent, who acts and makes decisions on behalf of the relying party. The delegation trust can be seen as a special case of the provision trust, because the relying party trusts the delegate not to misuse the delegated rights.
- **Identity trust** describes the belief that the claimed identity of an entity is true.
- **Context trust** describes the extent to which the trusting party believes that the distributed system contains mechanisms necessary to support the transaction in a case something goes wrong.

## 3. Traditional and Ad Hoc Grid Security

The purpose of any grid security infrastructure is to protect shared resource from malicious actions of users and user's data from unauthorized access. The common security mechanisms utilized for the protection purposes are the processes of authentication and authorization. However, the security in the traditional and ad hoc grid infrastructures is implemented in a different manner in regard to the architectural aspects of both grid technologies. The subsections 3.1 - 3.3 explain this issue in more details.

### 3.1 Traditional Grid Security Mechanisms

The first traditional grid infrastructures were used by a small group of users with unnamed trust relationships among them. When the community of users grew bigger, the need for secure access to resources, secure communication and data manipulation has become an important issue. The grid developers proposed and implemented several authentication and authorization infrastructures as a solution to this problem. The following subsections contain a brief survey of the most widely known and/or used infrastructures.

**Authentication infrastructures.** The process of authentication checks whether or not the identity of an entity is right. Probably the most known authentication infrastructure is the **Public Key Infrastructure** (PKI)[26], which is based on the concept of public key cryptography. The trust in a user's identity is established through a trusted third party, thus a pre-established trust relationship between the third party, grid users and resource providers is assumed. The trusted mediator is called Certificate Authority and is responsible for allocating the user's home domain identity into the grid identity and for issuing certificates with the allocated identity. The

issued certificates are used by the users as a means to authenticate to the resources shared in the grid community.

**Kerberos**[20] is another security infrastructure used for authentication of user's identity and is also based on pre-established trust relationships. The role of the trusted mediator is performed by the authentication server. The trust in the user's identity is mediated with session keys issued by the Authentication Server acting as the trusted third party. For the purpose of accessing the available services the Kerberos infrastructure uses special access tokens that carry the information about the identity of an entity and the groups to which the entity belongs.

**Athens**[4] is an authentication infrastructure developed to control access to a wide range of shared resources. Users have an account for each resource they wish to access and these accounts are managed centrally by the Account Server. An agent enforcing access control is installed in every site sharing resources. The user provides his user name and password in order to be granted the access to the requested resource. This step is repeated every time the user wants to access an available resource.

**Authorization infrastructures.** With the growth of grid popularity the enforcement of access control based only on user's identity become insufficient and more fine-grained access control was necessary. The process of authorization is used to determine who is allowed to use shared resources and under what conditions, whereby the user's identity (and other user's attributes) is considered before the final decision whether or not to allow the access to a particular resource is made. **Grid-Map Files** (GMFs) [14] is the first access control infrastructure based not only on user's identity. The main idea behind GMFs is the usage of access control lists. A list pairing distinguished names of authenticated grid users and local user accounts, to which these names are mapped, is stored on each shared resource. It is then left to the resource operating system and application access control mechanism to enforce the access to the resource.

**Virtual Organization Membership Service** (VOMS) [2] mediates trust between users and resource providers through a trusted third party - VOMS server. All information about a user is managed on the VO level by the VO administrator centrally. The VOMS server provides the user with attributes needed to access a shared resource in the form of attribute certificate. The user presents his attribute certificate issued and signed by VOMS server to a resource in order to access it. The resource checks the validity of the certificate and the attributes it contains. Subsequently, local resource access policies are applied and the user is granted or refused the access to the resource.

Another example of an authorization infrastructure is **PrivilEdge and Role Management Infrastructure Standard** (PERMIS)[6]. In order to access a resource protected by the PERMIS infrastructure the user needs to present a role based attribute certificate. The attribute certificate is issued by a source of authority and contains the user's role and attributes. PERMIS enables distributed role management, whereby certificates can be stored locally on the sites that allocated them. Before a decision whether or not to allow an access to a resource is made, the resource checks the user's certificate, role assigned to the user, and whether the certificate was issued by a trusted source of authority. Then the user is granted or refused the access to a requested resource.

The **Akenti**[1] infrastructure defines a special type of trusted entities called stakeholders. The stakeholders are trusted to issue use-condition certificates, which place conditions on certificates the user has to obtain in order to gain access to a resource. Every stakeholder can define use-condition certificates independently from other stakeholders. Hence, one resource can be protected by more access control requirements.

### 3.2 Ad Hoc Grid Security Mechanisms

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[15]. The security mechanisms described in the section 3.1 are unable to provide this type of protection.

Authentication and authorization, which are referred to as hard security mechanisms, do not allow any occurrence of risk or uncertainty (the user either is 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 is used as a mechanism for managing the 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[8, 15].

### 3.3 Traditional and Ad Hoc Grid Security Comparison

The traditional grid applications are hindered by the lack of security assurance from remote sites providing computing resources or other services. Trust models implemented in the grid environments support the user authentication and the single sign-on operations. However, the existing mechanisms are still inadequate to access local security conditions at sites participating in the grid community[22]. The situation in the ad hoc grid environments is similar. Grid nodes must assert the trustworthiness of a remote node according to the past experiences with the particular node and other considerable factors before the decision about the collaboration can be met.

In the traditional grid security infrastructures the identity trust, access trust and delegation trust are implemented as the processes of authentication, authorization and del-

| Characteristic | Grid type | |
|---|---|---|
| | Traditional | Ad hoc |
| Goal of grid security | Protection of shared resources and user's data from unauthorized access. | Protection of provided resources from malicious actions of users and protection of users from those providing the resources. |
| Prerequisites for provision of security services | Authentication of user's identity, secure communication and data transfer based on various cryptography technologies. | Authentication of collaborating entity's identity, secure communication and data transfer based on various cryptography technologies. |
| Provision of security services | Provision of security services is based on authentication and authorization mechanisms. | Provision of security is based on trust management. |
| Type of trust relationship | Implicit and unnamed trust relationships among grid community participants mediated through trusted third party. | Explicit trust relationship among ad hoc grid entities managed by each entity independently. |
| Supported trust classes | Identity trust as process of authentication, access trust as process of authorization and delegation trust as single sign-on operations. | Mutual trust relationship between two grid entities based on trust supporting all defined trust classes. |

**Table 1: Comparison of the traditional and ad hoc grid security characteristics**

egation of rights among the grid sites. Explicit implementations of the provision trust and context trust are missing. The proper behaviour of the resource provider and the user is guaranteed only by the third party acting as a trusted mediator. However, the trusted third party has no real mechanisms to ensure such behaviour.

In the traditional grid infrastructures trust is coupled with the establishment of the grid environment and is understood as an implicit part of the collaborations. On the other hand, in the ad hoc grids there are no implicit trust relationships among grid nodes. In the future the trust management mechanism could become responsible for the execution of collaborations in a presence of mutual trust.

The traditional and ad hoc grid security share a couple of similar features, e.g. the process of authentication is a prerequisite for other provided security services. However, the traditional and ad hoc grid security also differ in various characteristic features in regard to the grid architecture and the security needs of grid community participants. The most significant security characteristics of the both grid technologies are listed in the Table 3.3.

## 4. 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 behaviour. 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 the Fig. 1 introduces the trust manager module as a solution to meet the imposed requirements.

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[23, 22], 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 requirements filtering are assigned a trust index [23, 22] 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 as depicted in Fig. 2. The trust index is a combination of more parameters, but what 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 dependant 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 trust-

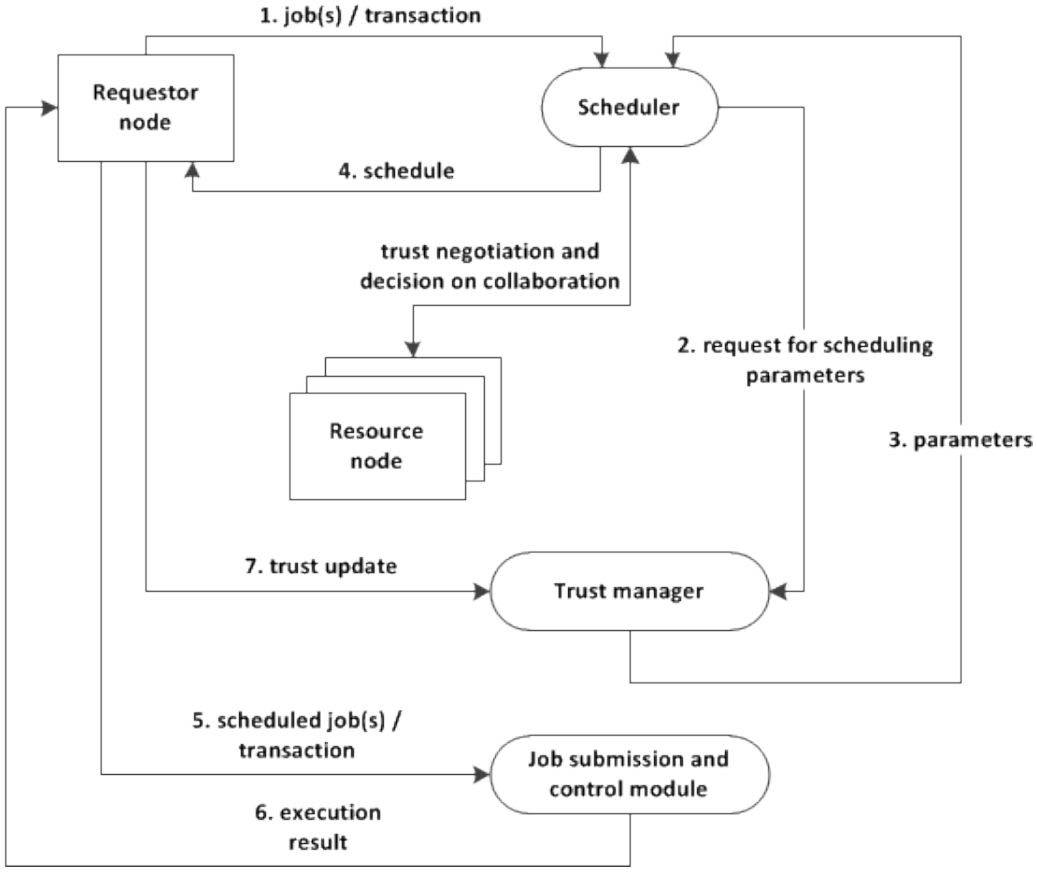


**Figure 1: Trust manager integration into the ad hoc grid infrastructure from the requester's point of view**

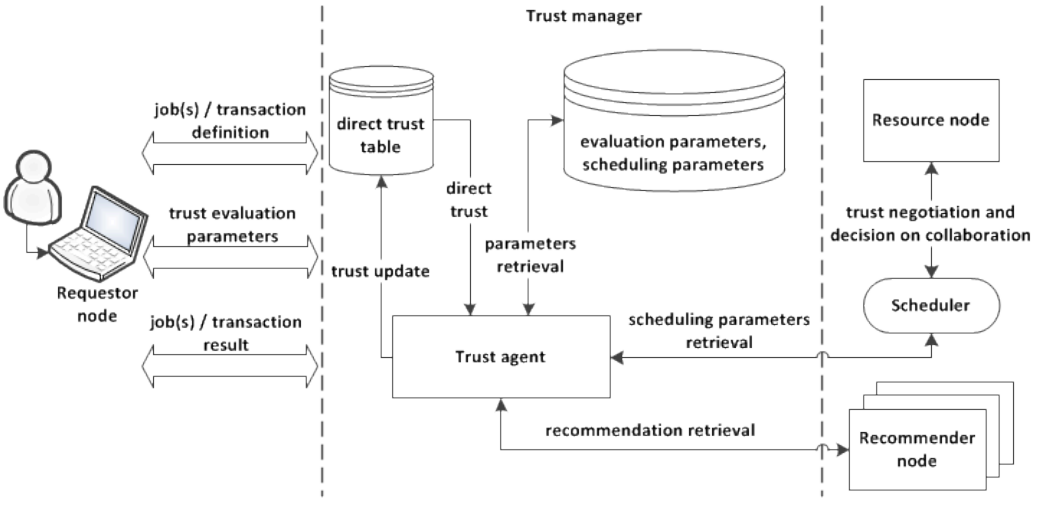


**Figure 2: Trust manager architecture from the requester's point of view**

worthiness 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 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.

## 5. 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 behaviour that can take form of user's program containing malicious code capable to compromise the resource provider's node or it can take a form of a malicious resource node capable to harm the user's job running on the provided resource [18].

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.

### 5.1 Parameters Classification

The user and the resource provider have different requirements for the grid security infrastructure. The user is interested in competence of the shared resources to reliably execute the user's code and to protect his data from unauthorized access or modification. Similarly, the resource provider wants to collaborate only with reliable and authenticated users not compromising the shared resource or the integrity of unauthorized data.

Each participant of a 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 were 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 components (as depicted in Fig.3): *(i)* behavioural parameters, *(ii)* system attributes *(iii)* and descriptive attributes.

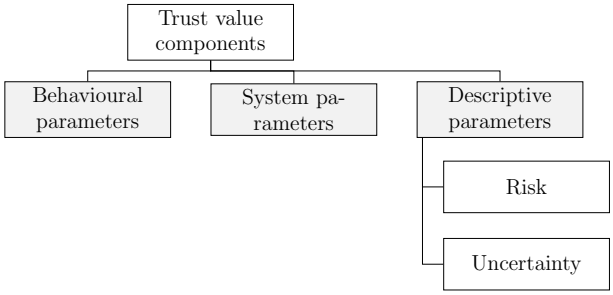


**Figure 3: Trust value components**

**Behavioural parameters** (e.g. accessibility, availability, competence and reliability) describe the behaviour of collaborating entities and are used to create history of data obtained from past interactions. By analysing the history of the collected data using statistical methods together with the entity's personalized notion of normal or anomalous behaviour 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 behavioural and system attributes the **descriptive parameters** (e.g. benefit and loss associated with a particular collaboration, amount of observed behavioural 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.

### 5.2 Determining Trust From Parameters

As already stated, 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 dependant on the risk and uncertainty (as depicted in Fig.4) 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 is the less certain about a collaboration execution the relying party

becomes. Therefore, the required level of security assurance increases as well.

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. There exist two alternative relations between trust and risk: risk determining level of trust and trust determining level of risk. The first relation can be described as follows: in a particular situation or a particular action with a certain level of risk a principal should be trustworthy in order to be allowed to enter the situation or carry out the action, i.e. the level of risk determines the minimal level of required trustworthiness. The latter relation is described as follows: in a particular situation or a particular action involving a principal with a certain level of trustworthiness the risk should be low enough in order to allow the principal to enter the situation or carry out the action, i.e. the level or trustworthiness determines the maximal level of acceptable risk. The letter view seems more appropriate for the risk evaluation if the costs and benefits of the entered situation are quantifiable [8].

The measurable parameters used for inferring the value of risk as depicted in Fig.4 are [16, 8, 17]:

- **Cost of a collaboration** represents the price (e.g. charges for using a shared resources) a relying party has to pay, if the transaction with a collaborating party will be launched. Typically, the relying entity is not willing to invest a large amount of funds in the collaboration unless the security assurance of the collaborating party is high. Therefore, the risk perceived by the relying party increases with the growing amount of investments.

- **Benefit** is the estimated gain (e.g. result of a data procession) obtained by the relying party after a successful execution of a collaboration. The greater the profit the more the relying party is motivated to launch a collaboration. Therefore, the risk perceived by the relying party decreases with the growing profit estimation.

- **Loss** describes the amount of funds the relying entity will lose in case of failure. The loss is not equal only to the paid cost, but also includes the estimated benefit, lost investment of time, importance of information or data obtained through collaboration, etc. Typically, the relying party is not willing to launch a collaboration coupled with a high loss unless the security assurance of the collaborating party is high. Therefore, the risk perceived by the relying party increases with the growing loss rate.

- **Necessity** of a collaboration execution describes a situation, in which the relying party needs to launch a collaboration in order to avoid certain or highly probably losses, even though negative consequences are possible. A high necessity of a collaboration lowers the required level of security assurance provided by the collaborating party. Hence, the risk perceived by the relying party decreases with the growing rate of a collaboration necessity.

**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 lack of information must not necessarily result in a change of trust in the trusted entity, but it can change the certainty about the final decision. However, if the certainty is changed significantly, the level of trust is changed as well [8].

The measurable parameters used for inferring the value of uncertainty as depicted in Fig.4 are:

- **Count of observations** refers to the amount of data describing the behaviour of collaborating parties obtained from past interactions. With the growing rate of collaborations the knowledge about the behaviour of collaborating parties becomes more accurate. Therefore, the relying party can be more certain about the decisions based on this knowledge.

- **Time passed since the last collaboration** determines certainty of the relaying party about its decisions. The certainty will be low, if the last interaction with a collaborating entity took place a long time ago or no collaboration was performed at all. On the other hand, if the last collaboration took place only recently, then the certainty will be high.

**Trust index**, which specifies the trustworthiness of a collaborating party, is dependant on direct trust and recommendations (as depicted in Fig.5). **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 dependant on the weights assigned to these two parameters.

As depicted in Fig.5, the parameters used for inferring direct trust are:

- **Basic trust** represents the degree to which the relying party is willing to trust a collaborating entity. Before collaboration with an unknown entity

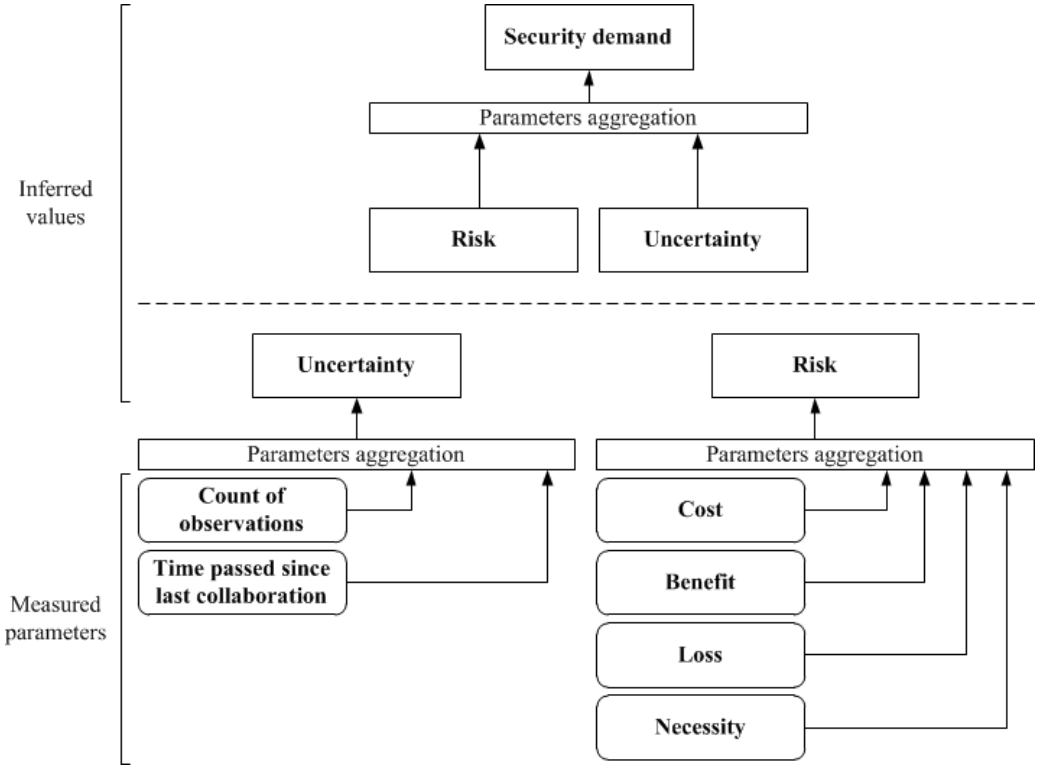


**Figure 4: Security demand inferred from trust components**

the relying party assigns to that entity an initial basic trust, which characterizes the entity as half-trusted and half-untrusted. After each collaboration the value of basic trust is updated with new value that is equal to the recalculated value of trust index. Basic trust also changes over time. The more time passed since the last collaboration, the more the value of basic trust approaches its initial value.

- **Aggregated attributes** represent the characteristics of collaborating entity relevant for trust evaluation. The attributes are aggregated into a single value corresponding to the quality of system resources offered by the entity and to the quality of entity's behaviour experienced over multiple collaborations.

- **Uncertainty** represents the amount of available information needed by the relying party to make an accurate decision on whether or not to launch a collaboration with a particular entity. Uncertainty affects the inferred value not directly. It only determines which parameter has greater influence on the inferred value (basic trust has higher influence in case of low uncertainty and aggregated attributes affect the inferred value more in case of high uncertainty).

The **aggregated attributes** (as depicted in Fig.5) are inferred from system and behavioural 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 behavioural attributes in case of high uncertainty and the behavioural attributes affect the inferred value more significantly in case of low uncertainty.

Concrete value of aggregated attributes can be inferred from the following system attributes (as depicted in Fig.5):

- **Identity** describes the quality of mechanisms used by grid entities to authenticate grid users and resource providers involved in collaborations mediated through the grid environment.

- **Privacy** corresponds to the capability of resource entity to allow access only to those system resources and data, which the authenticated user is permitted to use.

- **Security** corresponds to the general ability of resource entity to protect itself from harm that can be caused by jobs executing malicious code, malware programs or exchange of data over communication networks.

- **Data integrity** describes the ability of user's node and resource entity to prevent alteration of exchanged messages and data that can be avoided by protection of communication networks and by encryption of exchanged messages.

According the models dealing with behaviour trust [21, 19, 7] the behaviour of entity can be described with the following attributes (as depicted in Fig.5):

- **Accessibility** describes the capability of resource entity to respond to user's request for information retrieval about the state of the resource, the state of running user's job or for provision of other offered services.

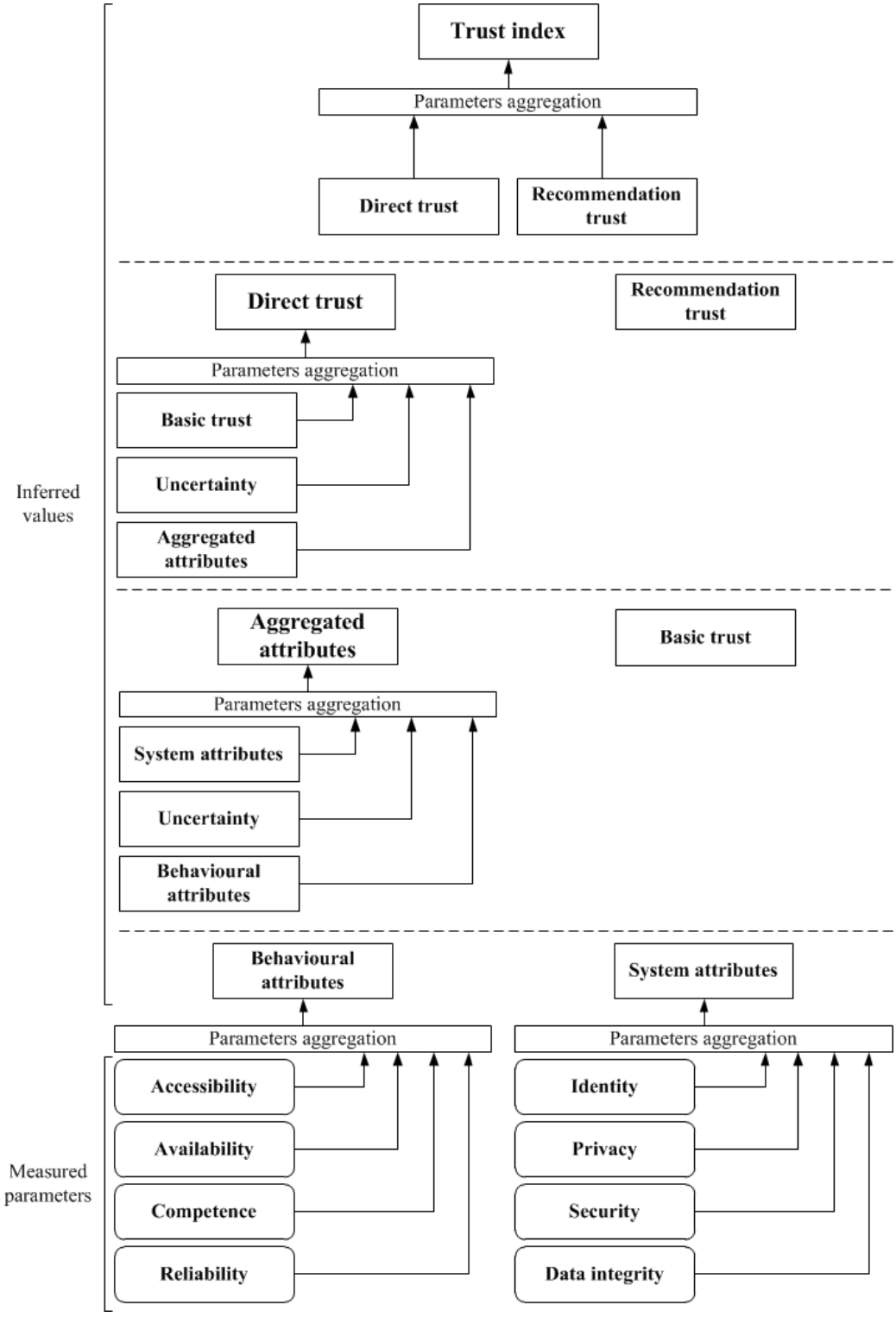


**Figure 5: Trust index inferred from trust components**

- **Availability** corresponds to the readiness of the resource to execute user's job, store data or provide other services offered by the resource provider.
- **Competence** from user's point of view corresponds to the readiness and willingness of resource node to provide all agreed system resources specified by the user and are part of the agreement between the user and the resource provider. From provider's point of view the competence describes the user's willingness to use only the agreed system resources and to use the provided resources only for the agreed amount of time.
- **Reliability** from user's point of view corresponds to the correct functioning of provided resource node or other services offered by the provider over a period of time. From provider's point of view the reliability describes proper execution of the user's program without compromising the provided resource node or altering unauthorized data.

## 6. 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[5]. The model of the ad hoc grid infrastructure executed by the simulation toolkit consists of ten user entities and ten resource provider entities. The modelled entities are assigned several system capabilities and forms of behaviour. The assigned capabilities and forms of behaviour are used for trust value calculation according to the model described in the section 5. The model also allows to schedule the user tasks according to the trust aware scheduling described in the section 4.

### 6.1 Experiment 1 – Ad Hoc Grid Without Trust Management

The first experiment was carried out by the simulation toolkit according to the modelled 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 modelled infrastructure. The values were used for comparison to values measured during other experiments.

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 table 2 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 task is 4880.36 (83.67% of all executed tasks) and count of failed tasks is 952.74 (16.33% of all executed tasks).

### 6.2 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 modelled ad hoc grid infrastructure with the incorporation of trust management. The table 3 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 task is 5292.12 (90.79% of all executed tasks) and count of failed tasks is 537.09 (9.21% of all executed tasks).

### 6.3 Evaluation Results

The verification of the modelled 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 modelled 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 modelled ad hoc grid infrastructure to support secure execution of user tasks. The reliability is measured as count of failed tasks observed during the simulation.

The figure 6 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 taks in a considerable manner. The figure 6 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 modelled ad hoc grid reliability is equal to 43.62%.

## 7. Future work

The requirements for the grid security can be mapped to various system, behavioural and descriptive attributes specifying the capability of a collaborating entity to execute activities in a secure manner. The task for the future research is to propose adjustments in the attribute weights resulting in reliability improvement of the proposed trust management integration.

The participants of the grid community usually have different requirements for the grid security. The diversity of the requirements necessitates the ability of the collaborating participants to define what system and/or behavioural attributes of interest should be included in the evaluated trust value. The participants should be able to assign weights to the evaluated attributes in order to specify the desired impact of the attributes on the evaluated trust value. The task for the future research is to design a mechanism giving the grid community participants ability to specify the evaluated attributes and their weights in an easy and understandable manner.

The infrastructure should also provide a well-defined application interface enabling an easy integration of trust management (i.e. trust evaluation, trust update and trust based decision making) into the current ad hoc grid solutions.

## 8. Conclusion

The decentralized structure and control independent nature of the ad hoc grid necessitates to manage the security

| Task type | Measured values | |
|---|---|---|
| | Count of executed tasks | 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 |

**Table 2: Count of tasks executed without trust management integration into the modelled ad hoc grid infrastructure**

| Task type | Measured values | |
|---|---|---|
| | Count of executed tasks | 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 |

**Table 3: Count of tasks executed with trust management integration into the modelled ad hoc grid infrastructure**

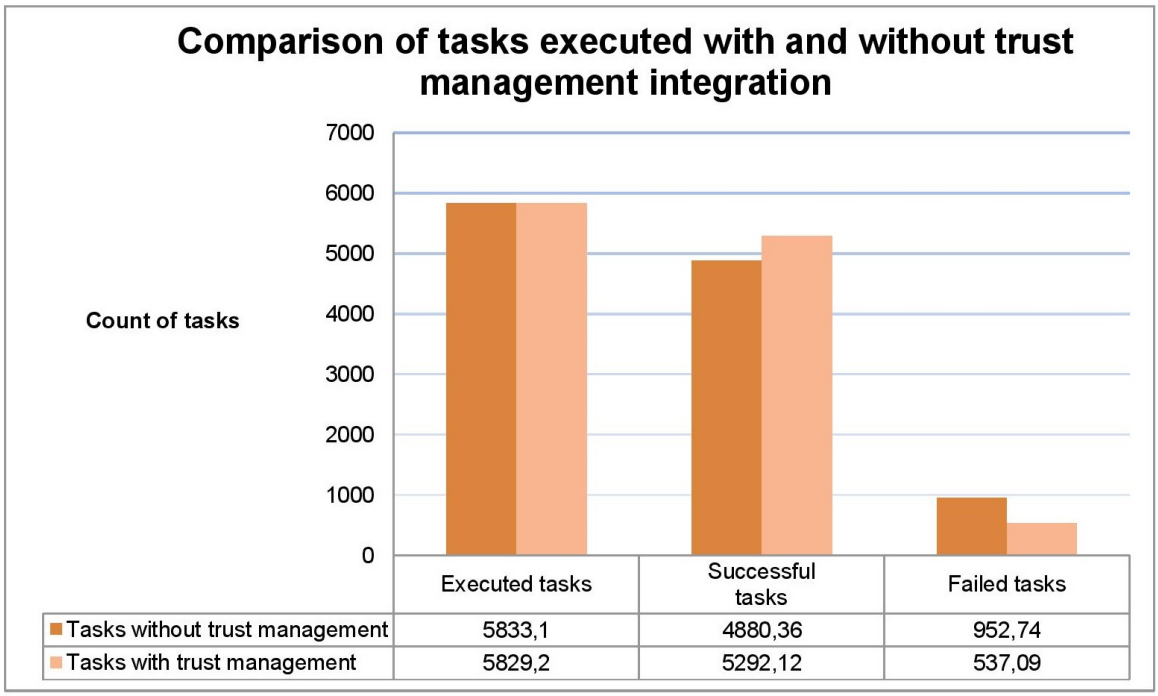


**Figure 6: Comparison of tasks executed with and without trust management integration into the modelled ad hoc grid infrastructure.**

in the absence of a central controller and the responsibility for the protection against malicious collaborators is left to the grid nodes. The issue of security provision in the ad hoc grid environment can be addressed with the integration of trust management into the scheduling process. However, the integration of trust management results in changes in the scheduling process and also necessitates enhancements in the ad hoc grid architecture. 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 behavioural 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 correctness of the proposed trust management integration. The paper also describes areas for future research dealing with refinement of the proposed solution and ease implementation of the proposed solution in the existing ad hoc grid infrastructures.

## References


[1] Akenti. [Online; http://dst.lbl.gov/ACSSoftware/Akenti/].

[2] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Gianoli, F. Spataro, F. Bonnassieux, P. J. Broadfoot, G. Lowe, L. Cornwall, J. Jensen, D. P. Kelsey, k. Frohner, D. L. Groep, W. S. de Cerff, M. Steenbakkers, G. Venekamp, D. Kouril, A. McNab, O. Mulmo, M. Silander, J. Hahkala, and K. LÃűrentey. Managing dynamic user communities in a grid of autonomous resources. *CoRR*, cs.DC/0306004, 2003.

[3] N. Andrade, L. Costa, G. GermÃşglio, and W. Cirne. Peer-to-peer grid computing with the ourgrid community. In *23rd Brazilian Symposium on Computer Networks (SBRC 2005) - 4th Special Tools Session*, 2005.

[4] Athens. [Online; http://www.openathens.net/].

[5] R. Buyya and A. Sulistio. Service and utility oriented distributed computing systems: Challenges and opportunities for modeling and simulation communities. In *Simulation Symposium, 2008. ANSS 2008. 41st Annual*, pages 68–81, April 2008.

[6] D. W. Chadwick, A. Otenko, and E. Ball. Role-based access control with x.509 attribute certificates. *IEEE Internet Computing*, 7(2):62–69, Mar. 2003.

[7] I. Dionysiou and H. Gjermundrod. sguts: Simplified grid user trust service for site selection. In *The Seventh International Conference on Internet Monitoring and Protection, 2012*, pages 40–46, May 2012.

[8] C. English, S. Terzis, and W. Wagealla. Engineering trust based collaborations in a global computing environment. In *Trust Management*, volume 2995 of *Lecture Notes in Computer Science*, pages 120–134, 2004.

[9] I. Foster, C. Kesselman, and S. Tuecke. The anatomy of the grid: Enabling scalable virtual organizations. *Int. J. High Perform. Comput. Appl.*, 15(3):200–222, Aug. 2001.

[10] I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell, and J. Von Reich. The open grid services architecture, version 1.5, July 2006.

[11] A. Gomes, A. Ziviani, L. Lima, and M. Endler. Performance evaluation of a discovery and scheduling protocol for multihop ad hoc mobile grids. *Journal of the Brazilian Computer Society*, 15(4):15–29, 2009.

[12] Gridbus. [Online; http://www.cloudbus.org/].

[13] Globus toolkit. [Online; http://www.globus.org/toolkit/].

[14] W. Jie, J. Arshad, R. Sinnott, P. Townend, and Z. Lei. A review of grid authentication and authorization technologies and support for federated access control. *ACM Computing Surveys*, 43(2):12:1–12:26, Feb. 2011.

[15] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644, mar 2007.

[16] A. Jøsang, C. Keser, and T. Dimitrakos. Can we manage trust? In *Trust Management*, volume 3477 of *Lecture Notes in Computer Science*, pages 93–107. Springer Berlin Heidelberg, 2005.

[17] A. Jøsang and S. L. Presti. Analysing the relationship between risk and trust. In *Trust Management*, volume 2995 of *Lecture Notes in Computer Science*, pages 135–145. Springer Berlin Heidelberg, 2004.

[18] C. Lin, V. Varadharajan, Y. Wang, and V. Pruthi. Enhancing grid security with trust management. In *Proceedings of the 2004 IEEE International Conference on Services Computing, 2004.*, pages 303–310, Sept 2004.

[19] P. Manuel, S. Thamarai Selvi, and M.-E. Barr. Trust management system for grid and cloud resources. In *First International Conference onAdvanced Computing, 2009.*, pages 176–181, Dec 2009.

[20] B. C. Neuman and T. Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38, Sept. 1994.

[21] E. Papalilo and B. Freisleben. Managing behaviour trust in grid computing environments. *Journal of Information Assurance and Security*, 3:27–37, March 2008.

[22] S. Song, K. Hwang, and Y.-K. Kwok. Trusted grid computing with security binding and trust integration. *Journal of Grid Computing*, 3(1-2):53–73, 2005.

[23] S. Song, K. Hwang, and M. Macwan. Fuzzy trust integration for security enforcement in grid computing. In *Network and Parallel Computing*, volume 3222 of *Lecture Notes in Computer Science*, pages 9–21. Springer Berlin Heidelberg, 2004.

[24] P. G. S. Tiburcio and M. A. Spohn. Ad hoc grid: An adaptive and self-organizing peer-to-peer computing grid. In *IEEE 10th International Conference on Computer and Information Technology (CIT)*, pages 225–232. IEEE Computer Society, 2010.

[25] Uniform interface to computing resources. [Online; http://www.unicore.eu/].

[26] J. Weise. Public key infrastructure overview, 2001. [Online; http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf].


## Selected Papers by the Author


S. Kavecký. Trust based grid security and security models. *International journal on information technologies and security*, ISSN 1313-8251, 4(3): 81–91, 2012.

S. Kavecký. Ad hoc grid trust management architecture. *International journal on information technologies and security*, ISSN 1313-8251, 5(3): 21–30, 2013.

S. Kavecký. Grid security and trust management overview. *IJCSI International journal of computer science issues*, ISSN 1694-0784, 10(3): 225–233, 2013.

S. Kavecký, P. Martincová. Overview of trust models integrating trust management into grid computing. *International journal of computer applications*", ISSN 0975-8887, ISBN 973-93-80889-96-8, 129(7): 1–6, 2015.

S. Kavecký, P. Martincová. Specification of parameters relevant for trust evaluation in an adhoc grid environment. *International journal of computer applications*", ISSN 0975-8887, ISBN 973-93-80889-96-8, 132(11): 1–8, 2015.

S. Kavecký, P. Martincová. A survey on trust aware security and scheduling in traditional and ad hoc grids. *International journal of computer applications*", ISSN 0975-8887, ISBN 973-93-80889-96-8, 133(12): 1–13, 2016.