Towards a VO Intersection Trust Model for Ad hoc Grid Environment: Design and Simulation Results

Ladislav Huraj, *Member, IAENG*, Vladimir Siládi, Jarmila Škrinárová and Veronika Bojdová

***Abstract*— An ad hoc grid environment is a spontaneous organization of cooperating heterogeneous nodes in a logical community without a fixed infrastructure and with only minimal administrative requirements. Trust is an integral part of ad hoc grid computing systems as well. It is not possible to utilize trust principles of traditional grid environment uses various, mostly centrally oriented methods for trust establishment, e.g. certification authorities, VO management servers or credentials pools. An ad hoc grid environment demands minimal administrative requirements; especially an absence of a central trust authority, where collaborating entities must establish and maintain a trust relationship among themselves.**

Our article presents a design of two algorithms for a supported authorization mechanism in order to more easily form virtual organizations based on attribute certificates. Moreover, an evaluation of the two algorithms, primary and extended algorithm, based on simulation results as well as deeper insights into the configuration of such schemes in ad hoc grid environment are described.

***Index Terms*—ad hoc grid, authorization, attribute certificates, VO intersection trust**

I. Introduction

An ad hoc grid environment binds varied idle computational resources to form a one-off grid for a particular grid job to provide computing resources on demand to every participant. Once the job is completed, the grid is disbanded. Ad hoc grid environment differs from traditional grids in their assumptions for trust-relationship, control-management, and technology support.

The ad hoc grid environment can be described as a spontaneous organization of cooperating heterogeneous nodes into a logical community without a fixed infrastructure. Every node in the network can spontaneously arise as a resource provider or a resource consumer at any time when it needs a resource or it possesses an idle resource. Moreover, the number of nodes within a system can increase; the participating nodes may have different ownership and varying use-policies. Therefore, it is required to develop new trust mechanisms to ensure that a malicious node cannot harm legitimate services running on the grid. Furthermore, research studies indicate that scheduling performance is affected by the heterogeneities of security and computational power of grid resources [1,17]. On the other hand, ad hoc grids demand minimal administrative requirements; especially an absence of a central trust authority where collaborating entities must establish and maintain a trust relationship.

Examples of applications of ad hoc grids include, for example, disaster management, wild fire fighting, and defense operations. An ad hoc grid environment allows grid entities to spontaneously establish an ad hoc relationship, to dynamically contribute services to the grid, to join existing grids, and to invoke services offered by other nodes in the ad hoc grid. Ad hoc grids facilitate interaction in an autonomous way without requiring pre-configured environments or management policies. They support a large class of applications that cannot be normally supported by traditional grid environments. These applications include, for example, market-oriented applications, transient collaborations, sporadic interactions, and other community applications that require on-the-fly grid establishment and deployment [2].

The three main characteristics of an ad hoc grid environment can be summed up as [3]: Dynamics, Resources and Independence. *Dynamics*: The main characteristics of an ad hoc grid is its highly dynamic nature, which results from the frequently changing structure of underlying networks and virtual organizations due to members switching on and off, member mobility, and so on [4]. Note that virtual organization (VO) in a grid environment refers to a dynamic set of entities with similar interests defined around an organisational structure to share the computing resources (CPUs, storage space, data, software, expertise, etc.) regardless of geographical location.

Resources: Ad hoc grids have more available resources (than for example MANETs), such as higher communication and computational capacity, more stable connections, etc. [5].

Independence: Ad hoc grids can be defined as a distributed computing infrastructure offering structure-, technology-, and control- independent grid solutions. Structural independence reflects the ability to self-organize among its participant users, i.e. each member is responsible for itself and it is not possible to use the centralized administrative services as in a traditional grid environment. Technology independence reflects the ability to support multiple grid protocols and technologies. Control independence mirrors the ability to support administrative functionality without any central coordination [6].

Manuscript received September 13, 2012.

L. Huraj is with the Dept. of Computer Science, Faculty of Natural Sciences, University of SS. Cyril and Methodius in Trnava, 91701 Trnava, Slovak Republic (phone: 421-33-5565185; e-mail: ladislav.huraj@ucm.sk).

V. Siládi is with the Dept. of Computer Science, Faculty of Natural Sciences, Matej Bel University, 974 01 Banská Bystrica, Slovak Republic (e-mail: vladimir.siladi@umb.sk).

J. Škrinárová is with the Dept. of Computer Science, Faculty of Natural Sciences, Matej Bel University, 974 01 Banská Bystrica, Slovak Republic (e-mail: jarmila.skrinarova@umb.sk).

V. Bojdová is with Department of Statistics, Faculty of Business Informatics, University of Economics in Bratislava, Dolnozemská cesta 1, 852 35 Bratislava, Slovak Republic, (e-mail: veronika.bojdova@euba.sk)

In this article, we show by simulation the results of an efficiency of our two algorithms for support authorization mechanisms based on the intersection of virtual organizations in ad hoc grid environments. The mechanism can be used to build trust relationships during the VO formation phase between grid entities even in cases when standard solutions have failed.

This paper is organized as follows: First we present a short overview of trust models in an ad hoc grid environment. Then both algorithms of our authorization model based on a VO intersection are described. The next section presents various simulations of proposed mechanisms through ns2 simulator as well as the effectiveness of the approaches. The paper concludes with a short summary.

II. Related works

In traditional grid environments, there is usually a central administrative authority and the relationships between entities are pre-established and centrally monitored. The authority is trustworthy for all entities in the environment.

As mentioned above, in an ad hoc grid environment, there is an absence of a globally trusted authority and participating entities must explicitly establish and maintain a trust relationship among themselves [7]. Therefore, various security mechanisms are practiced in an ad hoc grid environment.

Kerschbaum et. al. [8] solves the question of trust and reputation for member selection in the VO formation phase. Relationships between users are a combination of previous performance and recommendation trust, i.e. the trust relationship between two participants is formed based on the past experience they had with each other. Each member must register with the Enterprise Network Infrastructure by presenting some credentials to obtain feedback ratings for other members with whom they experienced transactions. In the dissolution phase of each VO all members leave positive or negative feedback ratings with the reputation server for the other members with whom they have completed transactions. The system requires each transaction to be rated by the participants. But from the ad hoc grid point of view, the reputation service is centralized and, moreover, the solution is more peer-to-peer than grid oriented.

In [5] the authors recommend further security solutions to study and to adapt techniques from Mobile ad hoc networks (MANET) and peer-to-peer networks to facilitate authentication for untrusted nodes in ad hoc grids. On the other hand, they underline that some techniques suitable for MANETs, such as identity-based authentication and symmetric-key-based authentication, are not suitable for ad hoc grids, since ad hoc grids are at a higher layer than MANETs.

We describe existing authorization mechanisms in traditional as well as ad hoc grid environments in detail, for example, in [3, 9]. Categorization of trust management in grids as well as description of VO lifecycles including VO formation phase can be found e.g. in [10].

III. Overview of VO intersection model

In this Section we describe both algorithms, primary and extended algorithm, of grid authorization mechanisms based on attribute certificates.

An authorization situation occurs when a potential user requires resources from other users. In an ad hoc grid, the decision regarding access is up to the resource owner. At first the resource owner tries to find the potential user within the grid map file. If the user is not included there, the resource owner asks for the user's attribute certificates. After that the resource owner checks if the user is a member of the same VOs as the resource owner or if there are any trustworthy attribute authorities which have signed the certificates. If no use-conditions are found for a potential user, access to the resources is denied. Our mechanism allows other ways based on attribute certificates by which a user can establish trust when previously used methods were not successful. An attribute certificate is a data structure that binds information about the holder to the attributes that are assigned to them, and digitally signed by the issuing attribute authority.

Since there is no direct trust to any VOs of a potential user from resource owner, the user tries to satisfy the owner to accept one of its VOs as a trustworthy VO and to allow access to the resources. The idea is similar to the philosophy of a decentralized trust model Web of Trust where PGP users build paths of trust among themselves in a distributed manner and the system allows users to specify how much trust to place in a signature by indicating how many independent signatures must be placed on a certificate for it to be considered valid [11].

Our method is based on the list of trustworthy VOs. The resource owner gives the list of all its trustworthy VOs as well as the minimal number k of co-members to the potential user. It is up to the user to search in its own certificate storage for relevant attribute certificates issued by some trustworthy VOs and so indirectly confirming the trustworthiness of its VO. If there are several combinations of VOs, the user chooses a VO in which its role is closest to its requests for grid resources.

Our authorization mechanism requires two main conditions:

(i) attribute certificates need to be stored on the side of each participant,

(ii) the trust is formed based on past authorized information included in attribute certificates, i.e. on previous VO membership of the users.

The first condition (i) requires the storing of attribute certificates from previous transactions. Since there is no central database of the certificates, each user builds its own storage of its attribute certificates as well as all attribute certificates of all known co-members of VOs. In this way, it can list its co-members in a VO as well as prove it with attribute certificates signed by particular VO. Building such storing space does not present a problem in a grid environment. A similar philosophy of storage in a grid environment can be found for example in the authorization system Akenti [12]. Akenti caches all the certificates that it finds in order to reduce subsequent search time. It also caches the authorization decision as a capability certificate that contains the access rights of a user for a resource, so

that subsequent requests for the same resource by the same user require no repeated decisions.

The second condition (ii) is based on previous authorization information included in attribute certificates and the trust decision of the resource owner is based on attribute certificates presented by a potential user.

The potential user should prove the trustworthiness of its VO by presenting k co-members of its VO which are acceptable for the resource owner. The acceptance means that the co-members are also members of another VO that is trustworthy to the resource owner. The potential user proves this with their attribute certificates.

The trust for an unknown potential user's VO is derived from the trustworthy VOs. If the intersection of a potential user's VO and resource owner's VOs is non-zero, the VOs from the intersection can be used to establish the trust. The number of certificates belonging to the VOs in the intersection of the potential user's VO with the resource owner's VOs respectively must be greater or equal to the threshold value k, the primary algorithm in Fig. 2.

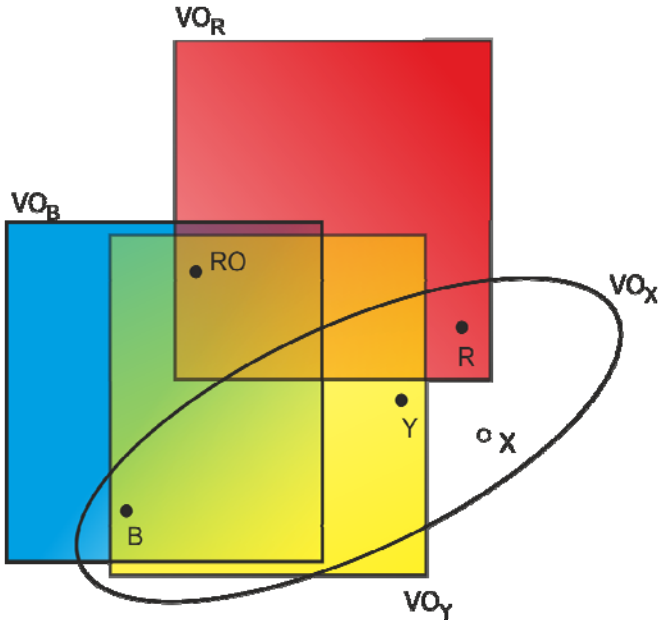

Fig. 1. Intersection of VOs. Users B, R and Y belong to trustworthy virtual organizations VO_B, VO_R and VO_Y respectively. RO establishes trust to VO_X from the VOs.

The value of the number k is based on the resource owner's policy. The higher k, the higher the resulting trust, on the other side, the lower k, the easier the feasibility of the authorization process. Moreover, the threshold value k can reflect the level of trust; the higher k allocates more rights, e.g. all the requested rights, the lower k allocates only particular rights.

Our mechanism does not assume any strictly pre-defined structure of trust, so such trust information is not in conflict with the independence of an ad hoc grid. On the other hand, the idea of the mechanism is based on the fact that ad hoc grid participants have previous authorization relations and they have collaborated in previous grid or ad hoc grid projects based on attribute certificates. If appropriate attribute certificates for confirmation of VO trustworthiness cannot be found on the potential user's side, the resource owner denies the access to the resource and other mechanisms of authorization and trust must be used.

For example, in the Fig. 1 there are three trustworthy virtual organizations VO_B, VO_R and VO_Y. The resource owner belongs to all the virtual organizations. Trust for VO_X is derived from the virtual organizations since users B, R and Y belong to the trustworthy virtual organizations as well as to the user's virtual organization VO_X. After the user X send k co-member certificates (k = 3) to RO, the RO check the certificates and can accept VO_X as a new trustworthy VO. Note if threshold value k = 4, the condition is satisfied as well, because user B belongs to two trustworthy virtual organizations, i.e. to VO_B and to VO_Y, and so user X can send four member certificates of trustworthy VO to the RO.

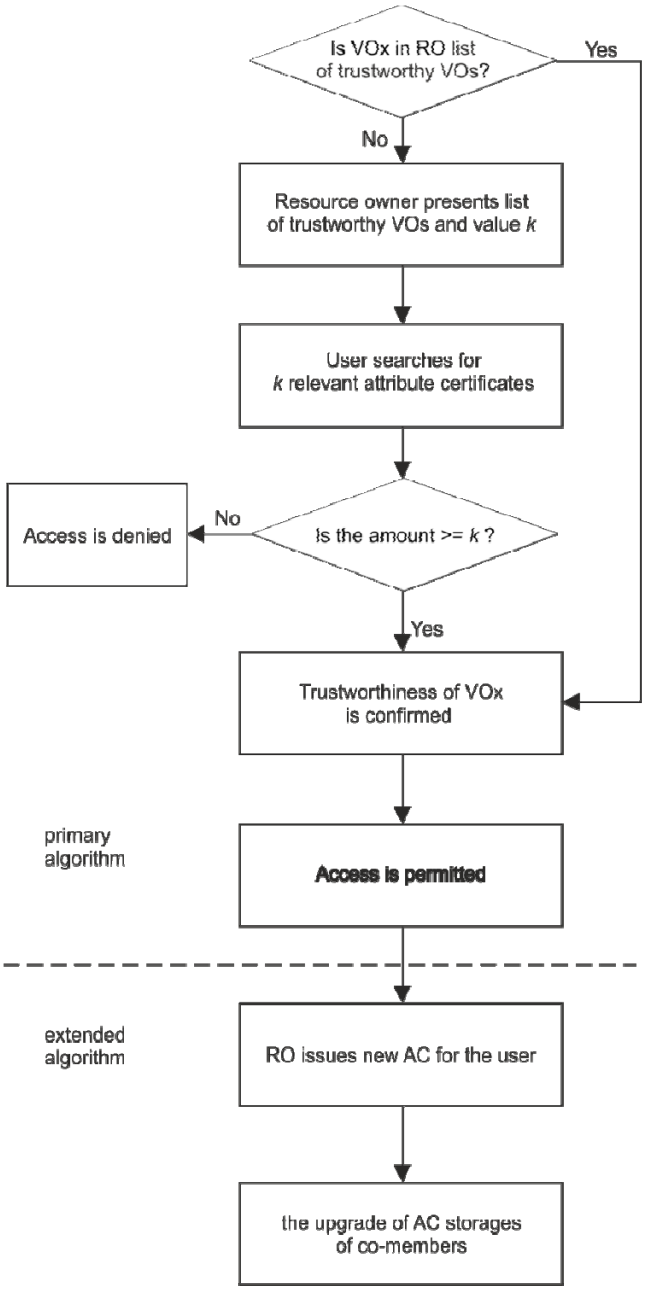

Fig. 2. Flow chart of the proposed VO Intersection Trust model. The trust for an unknown potential user's VO is derived from the trust to trustworthy VOs in the primary algorithm; after the acceptance of the user's VO by resource owner, the resource owner issues new attribute certificate in extended algorithm.

Extended version of the model

To achieve higher efficiency of the VO Intersection Trust model we try to extend the previous primary algorithm. Two steps are added to the model after the acceptance of the potential user's VO.

The resource owner has two possibilities: it can add the user or the user's virtual organization into its list of trustworthy users/VOs; or it can issue an attribute certificate with the set of rights for the user and thus include the user into its trustworthy entities. This certificate can be used in the future for further authorization decisions in the system as well.

Our extended algorithm uses the second possibility; see the extended algorithm in Fig. 2. After the acceptance of the user's VO by resource owner, i.e. the access to grid resources is permitted to the user, the resource owner issues a new attribute certificate.

Moreover, the new user's attribute certificate is distributed to several user's co-members, i.e. their attribute certificate storages are upgraded so they can utilize this certificate also during future authorization process.

IV. Performance Evaluation with Simulation Results

In our simulation to evaluate the performance of the authorization mechanism we used the Network Simulator 2 (ns2) written in C++ with OTcl interpreter, an object-oriented version of TCL. Ns2 was chosen as the base simulation engine due to the broad support. Moreover, in the simulation it is necessary to test only the dynamic as well as the independence of the scheme; the characteristic *Resources* of ad hoc grids can be neglected.

In ns2 simulation, a simulated application sits on top of transport agents connecting with other every 20 msec several times depending on the number of non-resource owner nodes (for each node once); the simulated applications have TCP as the underlining transport agents.

A fixed grid topology was used for all simulations as an initial setting. Presented topology consists of 20 grid nodes divided into four LAN connected to WAN through gateways, Fig. 3. It is possible to find similar use of the ns2 simulation for grid simulation, as well as analogous architecture topology in many other research works, for example in [13, 15].

Modifications of the initial simulation setting were tested in order to describe behavior of the model as well as to attain better efficiency of the schema. As it is described below, the efficiency of the extended algorithm depends on time period of the used algorithm, so we increased the number of connection to 300 times per 20 msec for randomly chosen nodes. On the other hand, for primary algorithm the number of connections does not have an impact on the efficiency of the proposed concept because the system does not upgrade particular information about new attribute certificates.

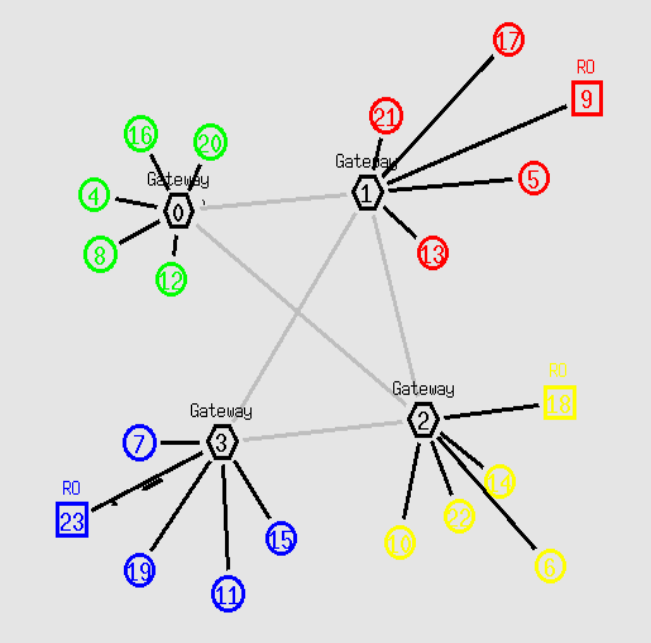

Fig. 3: Topology of the simulation; circles represent common nodes sending the requests for grid resources, squares are requested resource owners, hexagons are gateways.

A. First set of simulations – efficiency

We first investigated the behavior of the system with different parameter *k*. The parameter *k* is the number of required intersection nodes. Generally the *k* is chosen by each RO respectively. It is clear that no value will fit all the systems. Our goal was to investigate the practicability of the scheme for different value *k*. See Table 1 below.

TABLE 1
SIMULATION PARAMETERS FOR THE FIRST SET

Number of nodes 20
Number of resource owners: 10 %, 15 %, 20 %, 25 %, 30 %
Number of certificates for a node: randomly from 2 to 5
Rate of requesting users: 50 %
Threshold value *k*: 1, 2, 3, 4
Number of upgraded co-members: 4

In our simulation a randomly chosen node tries to contact a randomly chosen RO and to present its certificates and certificates of its co-members. The co-members of a requesting node were randomly chosen also.

We repeated the simulation 100 times for the 50% amount of the sending nodes representing more than 900 connections in the primary algorithm case and 30000 connections in the expanded algorithm case. The results for different value *k* (*k* = 1, 2, 3 and 4) are shown in Figure 4.

From the graph we note that our mechanism scales well to the ad hoc grid size and to *k* value. The results of both simulations confirm our assumption that the lower *k*, the easier the feasibility of the authorization process.

On the other hand, for *k* = 4, the system has more than 50% success of the trust establishment based on VO intersection, even for bigger 200 nodes' simulations [20]. Moreover, the results are relatively independent of the number of resource owners in the system and influenced only by the value k.

Additionally, the expanded algorithm shows extremely good results for value *k = 1* and *k = 2* for 300 times realized connection. As mentioned above, the efficiency decreases

with increasing of *k* value; even for *k* = *5* the efficiency of the expanded algorithm approaching to the primary algorithm. Increasing of efficiency for such bigger *k* values requires changing of some parameters of the model, as described later in the article.

B. Second set of simulations – amount of certificates

The second set of simulations investigated the efficiency of the mechanism following different numbers of accepted VOs by resource owner. In the simulation set we gradually increased a probability of accepted VOs by a resource owner, i.e. there was given a limit of the resource owner VO randomly chosen certificates. Number of nodes and ROs was fixed. The value *k* of required intersection nodes was assigned to two. We measured an average efficiency of 100 simulations for each setting, see Table 2.

TABLE 2
SIMULATION PARAMETERS FOR THE SECOND SET

Number of nodes 20
Number of resource owners: 15 %
Number of certificates for a node: randomly to 2, randomly to 3, randomly to 4, …, randomly to 12
Rate of requesting users: 50 %
Threshold value *k*: 2
Number of upgraded co-members: 4

The results of the second set of simulations are shown in Fig. 5.

It is apparent from Fig. 5 that the authorization mechanism based on VO interaction gives good results for all settings depending on amount of resource owner VOs for both algorithms.

As expected from intuition, the simulation results for primary algorithm indicate that generally, as the limit of resource owner VO certificates increases, the success of trust establishment increases, too. But already for limit 3 (i.e. a recourse owner accepts only one, two or three VOs), the average efficiency of the successful trust establishment achieved more than 50 %. After the limit 9 the value of the system showed only slight improvement and the success of trust establishment of the system was stabilized at around 89 %.

For the extended algorithm the results show good improvement of the scheme even for limit 2 (i.e. a recourse owner accepts only one or two VOs), the average efficiency of the successful trust establishment reached more than 88 % for that case. Efficiency of other, higher limits achieves in average the value around 93 %. The results indicate that applying of the extended algorithm of VO Intersection Trust model can rapidly support formation of virtual organizations based on attribute certificates even for small amount of co-members certificates, what makes the mechanism more appropriate for smaller ad hoc grids.

C. Third set of simulations – amount of upgraded co-members

The value of the amount of upgraded co-members in extended algorithm was in all previous simulations set to 4. And especially the efficiency of the extended algorithm for different amounts of upgraded co-members was tested in a herein described series of simulations, Table 3 below. The setting of the value to number 4 in previous simulations is based on obtained results from a series of simulations described in this Section.

Remember that the attribute certificate storage of some co-members of the user are upgraded after confirmation of trustworthiness of user's VO by resource owner and after issuing of new user's attribute certificate by resource owner, i.e. the new certificate is distributed to the co-members and they can use it as a relevant certificate for future trust

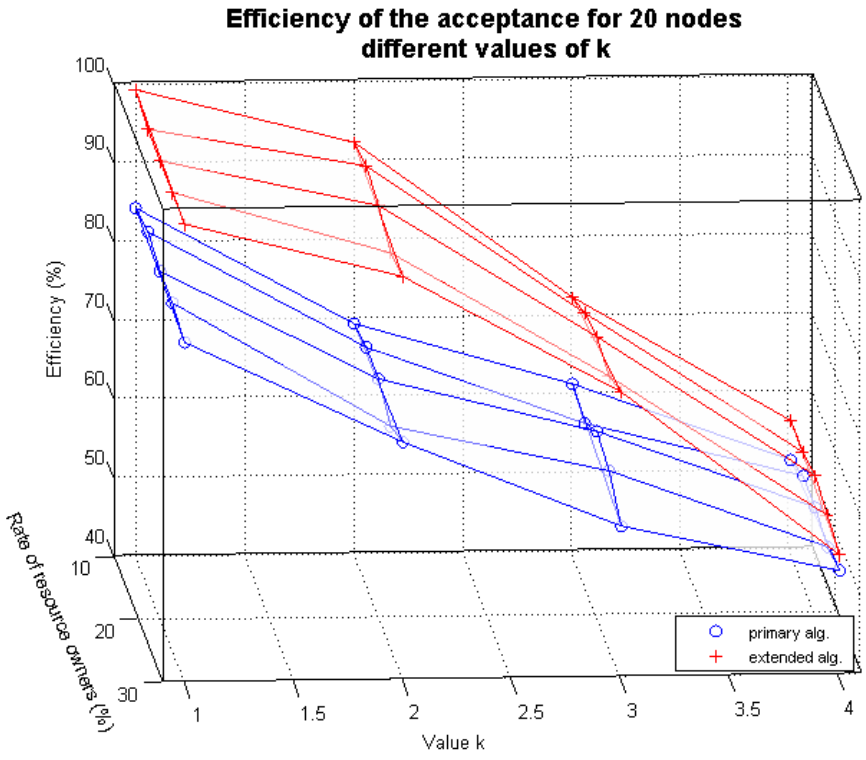

Fig. 4: Efficiency of the acceptance for 20 nodes; the number of required intersection nodes – parameter *k*, has been changed as well as the amount of ROs in the system.

negotiation which can increase the flexibility of the authorization scheme.

Note that if the amount of upgraded co-members in the simulation is set to 0 we obtain again the primary algorithm of the VO Intersection Trust model.

As can be seen from Figure 6, the efficiency of the scheme exceeds boundary 90 % for four upgraded co-members. Further increasing of upgraded co-members does make only insignificant benefit for this case.

TABLE 3
SIMULATION PARAMETERS FOR THE THIRD SET

Number of nodes 20
Number of resource owners: 15 %
Number of certificates for a node: randomly from 2 to 5
Threshold value *k*: 2
Number of upgraded co-members: 0, 1, 2, 3, 4, 5, 6, 7

We must further note that the upgrade of given number of co-members is not always possible, since in ad hoc grid environment not all co-members can be reachable at the same time and the real amount of the co-members may not be equal or higher to required number.

Not only the number of upgraded co-members can influence the resulting efficiency of the extended algorithm. Another argument which could also have an impact on the efficiency, could be the duration of the scheme. The behaviour of the extended algorithm for different durations is a matter of exploring of the next simulation series in the following section.

D. Fourth set of simulations – number of connections

In this part the extended algorithm is explored in detail in the point of algorithm duration and of its impact on the efficiency of the algorithm, Table 4.

TABLE 4
SIMULATION PARAMETERS FOR THE FOURTH SET

Number of nodes 20
Number of resource owners: 15 %
Number of certificates for a node: randomly from 2 to 5
Threshold value *k*: 2, 3
Number of upgraded co-members: 4
Period of the algorithm (connections per 20 msec): 20, 50, 100, 150, 200, 250, 300, 400, 500, 600, 700, 800

The results for a different value of k (k equal to 2 and 3) and a different amount of connections are shown in Figure 7.

From the graph it can be seen that if the system has enough formation time, the efficiency increases. For the value $k = 2$ the efficiency is close to 90 % for 200 connections; after 300 connections the efficiency is stabilized at value 93 %. As it was expected, for the value $k = 3$ the efficiency shows lower but still significant rate; the peak stabilized value of efficiency is 80 % for 600 connections; the efficiency for 300 connections is more than 73 %.

To enhance the efficiency, some interventions should be provided to algorithm setting or to authorization policies of RO; for example the 92% level of efficiency would be achieved for $k = 3$ for 600 connections too, if we increase the number of upgraded co-members (if it is in the scheme possible) three times.

In addition, the results of this simulation series indicate that in case where the user's request for grid resources was rejected because of lack of relevant certificates the user can try with a greater chance again to ask resource owner about the resource for acceptance after some time or eventually initiate re-establishment of the ad hoc grid with required resource owner after some time if the ad hoc grid is no longer obtainable.

V. STATISTICAL VALIDATION

In this Section statistical tests are performed to show the performance improvement.

The first set of simulations

We use the paired t-test to determine whether the improvement of a scheme based on an extended algorithm is significantly better than a scheme based on a primary algorithm. We compare two schemes in data points given in the Figure 4. Since each data point is the average of multiple simulation run results, we simply measure the results of the primary and extended algorithm in each run as the before and the after means respectively in order to get our t-test results.

Although we have a small sample size (of range 21), the differences (between values of efficiency for the extended and primary algorithm, shown in Figure 4) passed the normality test, so the t-test can be used.

We formulate the null hypothesis: "The scheme based on extended algorithm provides the same efficiency for 20 nodes for different values of k than the scheme based on primary algorithm" against the one-tail alternative: "The scheme based on extended algorithm provides higher efficiency for 20 nodes for different values of k than the scheme based on primary algorithm."

Table 5 shows the results of the t-test. It can be seen that the both of the p-values (for the two-tail and one-tail alternative hypothesis) are less than our significance level 0.01. The statistical results reject the null hypothesis, i.e. the scheme based on extended algorithm provides higher efficiency for 20 nodes for different values of k than the scheme based on primary algorithm (with a confidence level more than 99 %).

TABLE 5
T-TEST: PAIRED TWO SAMPLE FOR MEANS FOR THE FIRST SET

	algorithm	
	extended	*primary*
Mean	0.785566	0.65781
Variance	0.031383	0.015159
Observations	21	21
Pearson Correlation	0.949076	
Hypothesized Mean Difference	0	
df	20	
t Statistics	8.165288	
p-value (one-tail)	4.24E-08	
t Critical one-tail	1.724718	
p-value (two-tail)	8.49E-08	
t Critical two-tail	2.085962	

Furthermore, we reformulate the null hypothesis: "The difference between the mean efficiency of the scheme based on extended algorithm and the scheme based on primary algorithm is 10 %" against the one-tail alternative: "The difference between the mean efficiency of the scheme based on extended algorithm and the scheme based on primary algorithm is greater than 10 % (i.e. the scheme based on extended algorithm provides about 10% higher efficiency than the scheme based on primary algorithm)."

We use the paired t-test again, results are in Table 6. It can be seen that the p-value for our one-tail alternative hypothesis is 0.045649984. So we can reject the null hypothesis at the significance level 0.05. Hence the scheme based on extended algorithm provides about 10% higher efficiency than the scheme based on primary algorithm (with a confidence level 95 %).

TABLE 6
T-TEST: PAIRED TWO SAMPLE FOR MEANS FOR THE FIRST SET

	extended	*primary*
Mean	0.785565667	0.657810319
Variance	0.031382815	0.015158539
Observations	21	21
Pearson Correlation	0.949076177	
Hypothesized Mean Difference	0.1	
df	20	
t Statistics	1.773940695	
p-value (one-tail)	0.045649984	
t Critical one-tail	2.527976903	
p-value (two-tail)	0.091299968	
t Critical two-tail	2.845335985	

The second set of simulations

For the second set of simulations (shown in Figure 5) we use the Wilcoxon (paired) signed-ranks test, because of small sample size (of range 11) and violating the normality assumption. The Wilcoxon signed-ranks test is a non-parametric alternative to the paired t-test, which ranks the differences in performances of two classifiers for each data set, ignoring the signs, and compares the ranks for the positive and the negative differences. When the assumptions of the paired t-test are met, the Wilcoxon signed-ranks test is less powerful than the paired t-test. On the other hand, when the assumptions are violated, the Wilcoxon test can be even more powerful than the t-test.

As above, we formulate the null hypothesis: "The scheme based on the extended algorithm provides the same efficiency for 20 nodes for a different amount of RO certificates than the scheme based on the primary algorithm." against the one-tail alternative: "The scheme based on extended algorithm provides higher efficiency for 20 nodes for different amount of RO certificates than the scheme based on primary algorithm."

Table 7 shows the results of the test. It can be seen that the p-value=0.003346 is less than our significance level 0.01. So we can reject the null hypothesis, i.e., the scheme based on extended algorithm provides higher efficiency for 20 nodes for different amount of RO certificates than the scheme based on primary algorithm (with a confidence level more than 99 %).

TABLE 7
WILCOXON SIGNED RANKS TEST FOR THE SECOND SET

	algorithm	
	extended	*primary*
Mean	0.925799	0.741413
Std. deviation	0.018055	0.171918
Statistical test		
Measure	*Value*	
Used examples	11	
Sum ranks + (T+)	66	
Sum ranks - (T-)	0	
E(T+)	33	
V(T+)	126.5	
Z Statistics	2.934058	
p-value	0. 003346	

Both the paired two-sample for means t-test and the Wilcoxon signed-ranks test yielded a p-value < 0.001 or 0.05 for the measurements, which indicates the statistical significance of these results.

VI. CONCLUSION

We have designed a support VO intersection based on authorization mechanism for an ad hoc grid environment. In the mechanism, the indirect trust for a virtual organization is established based on the attribute certificates of *k* members which belong to trustworthy VOs. The mechanism can facilitate the building of trust relationships for the phase of VO formation for ad hoc grid environments in cases when standard solutions have failed and so to support authorization process.

Moreover, we have simulated and evaluated two versions of the authorization model, the primary algorithm and the extended algorithm. Our simulation results show the effectiveness of the proposed approach. Furthermore, we provided some detailed insights into the configuration and behaviour of such a scheme in ad hoc grid environments based on an ns2 simulator.

Two main parameters influence the efficiency of the primary algorithm of the proposed model. The first is the threshold value *k* given by a resource owner and describing the demand of intersection VO amount by resource owner. The second parameter includes numbers of accepted VOs by resource owner. While the first parameter is easily adjustable by resource owner, the second one depends on previous transactions of ad hoc grid entities.

Two more parameters influence the extended algorithm of the proposed model hence this version of the scheme is better scalable than the primary algorithm. The parameters are amount of upgraded co-members where the new certificate is distributed to the co-members; and the amount of connections during the algorithm process corresponding to the algorithm duration.

In summary, the measured results demonstrate that it is possible to scale the efficiency of the proposed VO Intersection Trust model by the parameters depending on authorization policy of particular entities in ad hoc grid; and furthermore as statistical tests have shown, during the appliance of the model the efficiency of proposed scheme increases.

Further extension of the work involves the revocation issue of the proposed mechanism and detailed testing from different points of view [14, 16, 18, 19] before being applied in practice.

REFERENCES

[1] Kashyap, R., Vidyarthi, D. P. Dual Objective Security Driven Scheduling Model for Computational Grid using GA, *IAENG International Journal of Computer Science*; 2012, Vol. 39 Issue 1, pp. 71-79.

[2] Li C, Li L. Design and implementation of economics-based resource management system in ad hoc grid. In: *Adv Eng Softw (2011)*, doi:10.1016/j.advengsoft.2011.10.003

[3] Huraj L., Siládi, V.: Authorization through Trust Chains in Ad hoc Grids. In: *Proceedings of the 4th ACM EATIS annual international conference on Telematics and Informatics: New Opportunities to increase Digital Citizenship (EATIS '09)*, Prague, Czech Republic, June 2009, pp. 68-71, ISBN 978-1-60558-398-3.

[4] H. Kurdi, M. Li, and H. Al-Raweshidy. A classification of emerging and traditional grid systems. In: *IEEE Distributed Systems Online*, 9(3), March 2008.

[5] S. Zhao, A. Aggarwal, and R. D. Kent. Pki-based authentication mechanisms in grid systems. In: *IEEE Int. Conference on Networking, Architecture, and Storage*, pp. 83-90, 2007.

[6] K. Amin, G. von Laszewski, and A. R. Mikler. Hot service deployment in an ad hoc grid environment. In: *Proc. of the IEEE 12th Int. Conference on Advanced Computing and Communications*, 2004.

[7] K. Amin, G. von Laszewski, and A. R. Mikler, Toward an Architecture for Ad Hoc Grids. In: *Proceedings of the IEEE 12th International Conference on Advanced Computing and Communications (ADCOM 2004)*, Ahmedabad Gujarat, India, December 2004.

[8] F. Kerschbaum, J. Haller, Y. Karabulut, and P. Robinson. Pathtrust: A trust-based reputation service for virtual organization formation. In: *iTrust2006, 4th International Conference on Trust Management*, Vol. 3986, Lecture Notes in Computer Science, pp. 193-205, Springer, 2006.

[9] Huraj, L., Reiser, H.: "VO Intersection Trust in Ad hoc Grid Environments". In: Fifth International Conference on Networking and Services (ICNS 2009), Valencia, Spain, IEEE Computer Society, April 2009, pp. 456-461

[10] Alvaro Arenas, Michael Wilson, Brian Matthews, "On Trust Management in Grids," Proceedings of the 1st international conference on Autonomic computing and communication systems, 2007 Article No.: 4.

[11] Khari, M., Shrivastava, G.: Public Key Infrastructure and Trust of Web Based Knowledge Discovery, In: *International Journal of Computer Science and Security (IJCSS)*, Volume 5, Issue 3, 2011

[12] M. R. Thompson, A. Essiari, and S. Mudumbai, Certificate based authorization policy in a PKI environment, In: *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 4, USA, November 2003, pp 566-588.

[13] N. Thenmozhi and M. Madheswaran: Analysis of impact of Symmetric Encryption Algorithms in Data Security Model of Grid Networks. In: International Journal of Computer Science and Information Security, Volume 8, Issue 6, 2010, pp. 99-106.

[14] Strémy, M., Eliáš, A.: Virtual laboratory communication. In: *Annals of DAAAM and Proceedings of DAAAM Symposium. - ISSN 1726-9679. - Vol. 20, No. 1 Annals of DAAAM for 2009 & Proceedings of the 20th international DAAAM symposium "Intelligent manufacturing & automation: Focus on theory, practice and education" 25 - 28th* November 2009, Vienna, Austria. - Vienna : DAAAM International Vienna, 2009. - ISBN 978-3-901509-70-4, pp. 0139-0140.

[15] J. C. Cunha and O. F. Rana. *Grid Computing: Software environments and Tools.* Springer Verlag, January 2006.

[16] Tanuska, P. and Skripcak, T.: The Proposal of Functional User Requirements Generation. In: *ICCRD 2011: 3rd International Conference on Computer Research and Development*. March 11-15, 2011, Shanghai, China. Beijing: IEEE, 2011. ISBN 978-1-61284-840-2. pp. 39-42.

[17] Simon, M. 2010. Deploying network intrusion detection system in process control networks. In Infokommunikacionnye technologii v nauke, proizvodstve i obrazovanii : Cetvertaja meždunarodnaja naučno-techničeskaja konferencija. Stavropoľ : Izdateľstvo Severo-Kavkazskogo gosudarstvennogo techničeskogo universiteta. ISSN 2219-293X. Časť 1 (2010), s. 178-182.

[18] Šuch, O.: On families of additive exponential sums. In: *Finite Fields and their Applications*, 11 (4), 2005, pp. 700-723.

[19] Šuch, O.: Vertex-transitive maps on a torus. In: *Acta Mathematica Universitatis Comenianae*, 2011, 80 (1) , pp. 1-30.

[20] Huraj L., Siládi, V.: Evaluation of VO Intersection Trust model for Ad hoc Grids. *Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2012*, IMECS 2012, March 14-16, 2012, Hong Kong, pp. 213-217, ISBN: 978-988-19251-1-4

Ladislav Huraj received the Ph.D. degree in Applied Informatics from the Slovak Technical University, Faculty of Electrical Engineering and Information Technology, Slovakia in 2006. He is currently a Head of the Department of Computer Science and Mathematics at The University of SS. Cyril and Methodius in Trnava, Slovakia. Dr. Huraj's research interest is primarily in Grid Computing, Information Security and Computer Education.
He is a member of Slovak Association for Information Security SASIB, ACM member, IAENG member and an editorial board member of Journal of Convergence Information Technology.

Vladimír Siládi received his M.S. degrees in Mathematics, Computer science, pedagogy of basic and secondary schools from Matej Bel University, Slovak Republic, in 1993. Since he received PhD. degree in Computer hardware and systems from Slovak University of Technology, Slovak Republic, in 2007. He is an assistant professor of the Department of Computer Science at Matej Bel University. His research interest is primarily in Parallel computing architectures, Grid Computing, Computer Education. He is a member of ACM, SISp (Slovak informatics society), SSAKI (Slovak Society of Applied Cybernetics and Informatics), JSMF (The Union of Slovak Mathematicians and Physicists).

Jarmila Škrinárová received her engineer diploma degrees in from Slovak University of Technology, Slovak Republic, in 1986. Since she received PhD. degree in 2004 from Slovak University of Technology, Slovak Republic, in Automation and Control, Cybernetics. She is a senior lecturer of the Department of Computer Science at Matej Bel University. Her research interest is primarily in Parallel computing, Grid Computing, Artifiacial Intelligence and Computer Education. She is a member of ACM, SISp (Slovak informatics society), SSAKI (Slovak Society of Applied Cybernetics and Informatics). She has been reviewer of IEEE conferences papers and IEEE journals. She is member of 24 conferences program committees. She is a local coordinator of the project -Slovak infrastructure for HPC at Matej Bel University.

Veronika Bojdová received the Ph.D. degree in Probability and Statistics from the Matej Bel University, Slovak Republic, in 2009. She is an assistant professor at the Department of Statistics at University of Economics in Bratislava.
Her research interest is primarily in Statistical Methods and Datamining.
She is a member of JSMF (The Union of Slovak Mathematicians and Physicists).

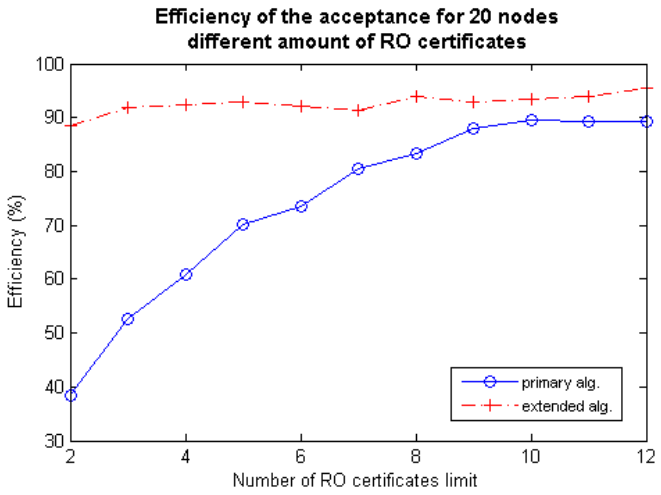

Fig. 5: Efficiency of the acceptance for 20 nodes; parameter *k*=2;
the limit of RO certificates has been changed.

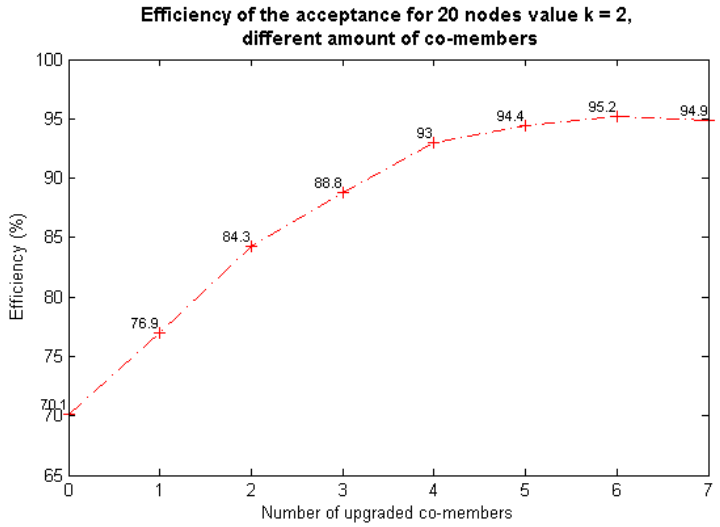

Fig. 6: Efficiency of the acceptance for 20 nodes for the extended algorithm; parameter *k*=2;
the amount of co-members has been changed.

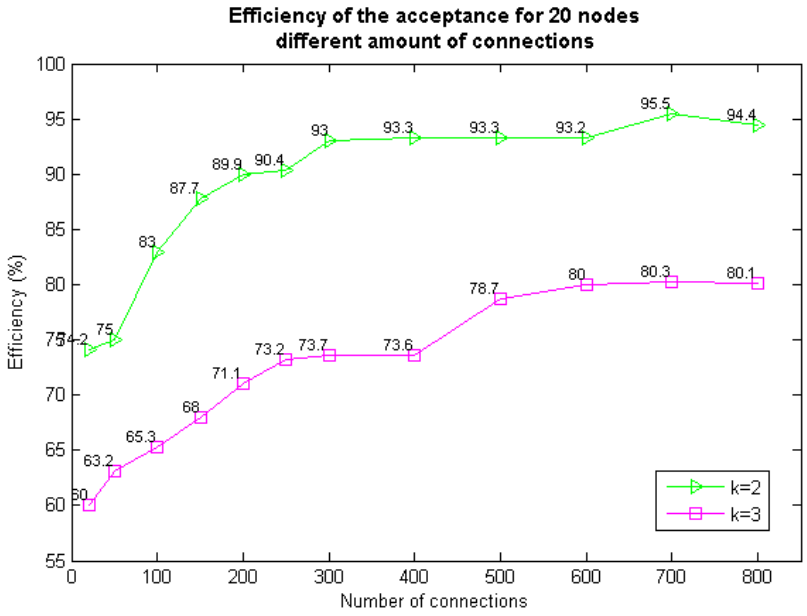

Fig. 7: Efficiency of the acceptance for 20 nodes for the extended algorithm; parameter k=2 and k=3;
the amount of connections has been changed.