Evaluation of VO Intersection Trust model for Ad hoc Grids

Ladislav Huraj and Vladimir Siládi

***Abstract*— Trust is an integral part of grid computing systems. Traditional grid environment uses various, mostly centrally oriented methods for trust establishment, e.g. certification authorities, VO management servers or credentials pools. On the other side, 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 among themselves. The paper presents a design of a supported authorization mechanism for easier formation of virtual organizations based on attribute certificates. Moreover, an evaluation of the mechanism based on simulation results as well as insights into the configuration of such scheme in ad hoc grid environment are described.**

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

I. Introduction

The ad hoc grid environment binds together 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 malicious node cannot harm legitimate services running on the grid. Furthermore, 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 among themselves.

Manuscript received December 07, 2011; revised January 18, 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).

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, dynamically contribute services to the grid, join existing grids, and 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 [1].

The three main characteristics of an ad hoc grid environment can be summed up as [2]: 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 [3]. Note that virtual organization (VO) in 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. [4].

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 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 [5].

In this article, we show by simulation the results of an efficiency of our support authorization mechanism based on intersection of virtual organization in ad hoc grids environment. The mechanism can be used to build trust relationships during VO formation phase between grid

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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 ad hoc grid environment. Then our authorization model based on VO intersection is described. Next section presents the simulation of proposed mechanism through ns2 simulator as well as the effectiveness of the approach. The paper is concluded 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 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 [6]. Therefore; various security mechanisms are practiced in ad hoc grid environment.

For example, Kerschbaum et. al. [7] solve 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 [4] authors recommend for 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 environment in detail for example in [2, 8]. Categorization of trust management in grids as well as description of VO lifecycles including VO formation phase can be found e.g. in [9].

III. Overview of VO intersection model

In this Section we describe grid authorization mechanism based on attribute certificates.

An authorization situation occurs when a potential user requires resources from others. 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 mapfile. 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 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 potential user, the access to the resources is denied. Our mechanism allows other way based on attribute certificates by which 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, 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 philosophy of 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 [10].

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 of 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) storing of attribute certificates 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 of 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 grid environment can be found for example in the authorization system Akenti [11]. 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.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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 trust to trustworthy VOs. If the intersection of potential user's VO and resource owner's VOs is non-zero, the VOs from the intersection can be used to establish the trust. Number of certificates belonging to the VOs in intersection of the potential user's VO with the resource owner's VOs respectively must be greater or equal to the threshold value *k*.

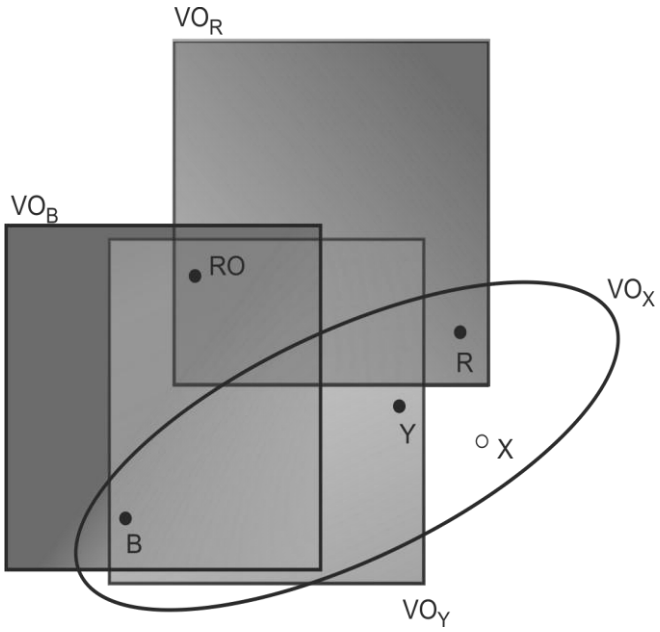

Fig. 1. Intersection of VOs. Users B, R and Y belong to trustworthy virtual organizations VO_B, VO_R and VO_Y respectively. RO establishes trust to VO_X from the VOs.

The value of the number *k* is based on resource owner 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-definite 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. 2 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 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.

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 50 ms; the simulated applications have TCP as the underlining transport agents.

A fixed grid topology was used for all simulations. Presented topology consists of 20 grid nodes divided into four LAN connected to WAN through gateways, Fig. 2. It is possible to find similar using of the ns2 simulation for grid simulation, as well as analogous architecture topology in many other works, for example in [12, 14].

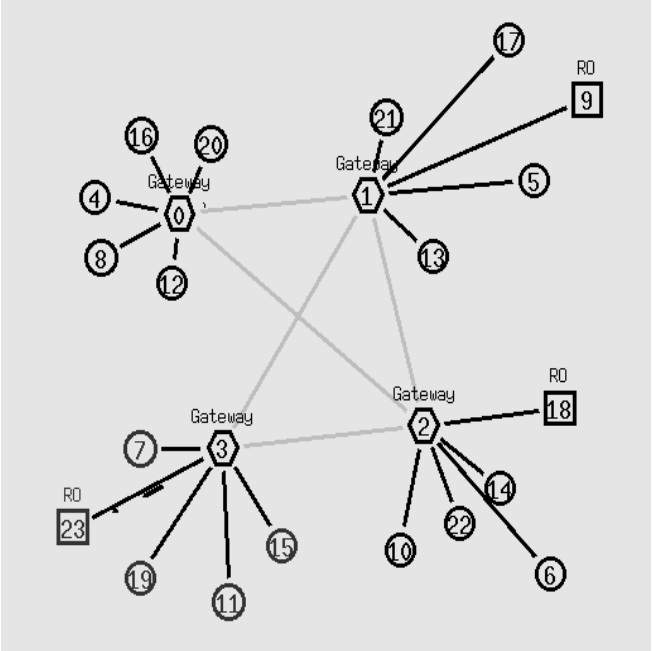

Fig. 2: Topology of the simulation; circles represent common nodes, squares are ROs, hexagons are gateways.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

A. *First set of simulations – efficiency*

We first investigated the behaviour 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*, Table 1.

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

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 what for the 50% amount of the sending nodes representing more than 1800 connections in a case. The results for different value *k* (*k* = 1, 2, 3 and 4) are shown in Figure 3.

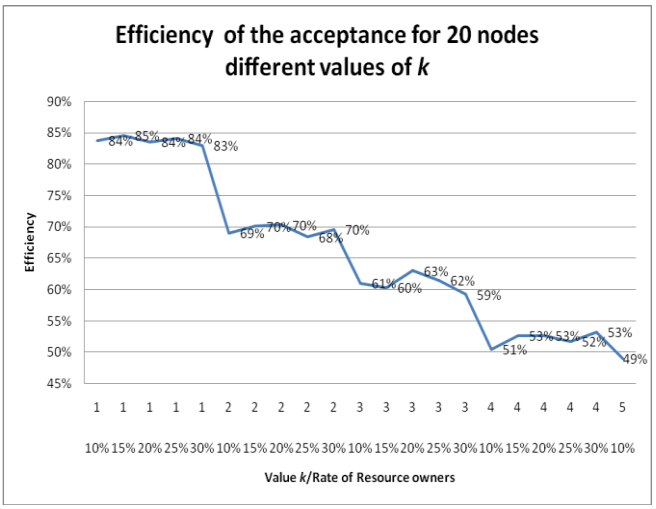

Fig. 3: Efficiency of the acceptance for 20 nodes; the number of required intersection nodes – parameter *k*, has been changed as well as the amount of ROs in the system.

From the graph we note that our mechanism scales well to the ad hoc grid size and to *k* value. The results of the simulation 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.

B. *Second set of simulations – amount of certificates*

The second set of simulations was oriented to investigate 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, 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

The results of the second set of simulations are shown in Fig. 4.

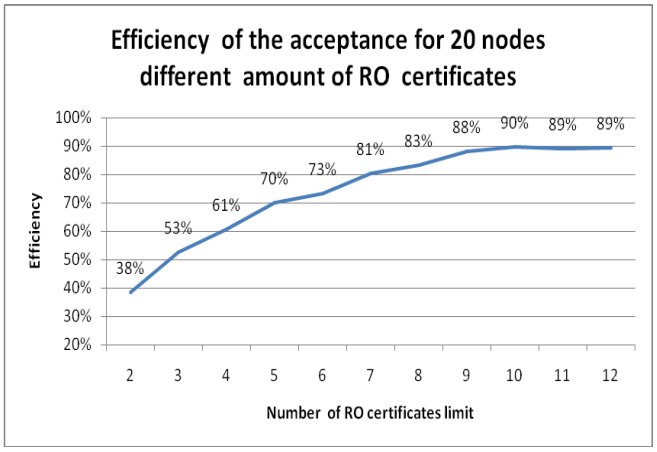

Fig. 4: Efficiency of the acceptance for 20 nodes; parameter *k*=2, the limit of RO certificates has been changed.

It is apparent from Fig. 4 that the authorization mechanism based on VO interaction gives good results for all settings depending on amount of resource owner VOs.

As expected from intuition, the simulation results 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%.

V. CONCLUSION

We have designed a support VO intersection based authorization mechanisms for an ad hoc grid environment. In the mechanism, the indirect trust for a VO 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.

Moreover, we have evaluated the authorization model by simulation results. Our simulation results show the effectiveness of the approach. Furthermore, we provided some insights into the configuration of such scheme in ad hoc grid environment.

Further extension of the work involves comparison of the scheme results with an extension where the resource owner

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

will add the new user's VO into the list of trustworthy VOs after the acceptance of the potential user. Also, the revocation issue of the mechanism and detailed testing from different points of view [13, 15] before being applied in practice should be investigated.

REFERENCES

[1] 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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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

[9] 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.

[10] 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

[11] 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.

[12] 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.

[13] 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.

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

[15] Tanuska, P., Moravcik, O., Vazan, P.: The base testing activities proposal. 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*, November 2009, Vienna, Austria. DAAAM International Vienna, ISBN 978-3-901509-70-4, pp. 371-372.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)