A Multicriteria Method for Evaluating Risks in Virtual Organizations

Rafael Giordano Vieira, Omir Correia Alves Junior and Adriano Fiorese
UDESC, State University of Santa Catarina
CCT, Department of Computer Science - DCC
89223-100, Joinville-SC, Brazil
e-mail:{dcc6rgv, dcc2ocaj, fiorese}@joinville.udesc.br

***Abstract*—The development of collaborative environments has become a key factor for Service Providers (SPs) successfully leverage their business activities. Nevertheless, the volatility of these networks leads to several additional risks, that need to be identified, measured, and mitigated through a well-defined process. In this way, this paper presents a supporting decision method that analyses the risk of a set of pre-selected SPs based on collaboration and infrastructure KPIs to compose Virtual Organizations (VOs). A computational prototype was also specified and used to execute a set of tests to assess the proposed risk analysis method. Results show the consistency of proposed method.**

***Index Terms*—Virtual Organization, P2P SON, Risk Analysis**

I. Introduction

Nowadays, the service provisioning is one of the major sources of revenue in the in the Internet as a whole. Particularly, the evolution of Peer-to-Peer Service Overlay Networks (P2P SONs) [1], [2] is providing a suitable environment for companies to make their services available to the global user community. The joining of the SON and P2P fields offers a high potential for handling services, by creating dynamic and adaptive value chain networks across multiple Service Providers (SPs). Moreover, a wide range of services can be made available, as well as an environment where price and quality can be competitive differentials [3].

The P2P SON concept applies to a broad range of network architectures. This paper deals particularly with the Virtual Organization (VO) one. A VO is a temporary and dynamic strategic alliance of autonomous, heterogeneous and usually geographically dispersed companies created to attend very particular business opportunities [4], [5]. In this sense, the P2P SON provides an environment for VO formation and, additionally, enhances benefits to its members (SPs), that is, sharing costs, bandwidth and others [1].

Although the mentioned advantages of using P2P SON can improve the VO formation process, the natural VO networked structure faces additional risks than other general forms of organization. These additional risks come, in part, from the increasing sharing of responsibilities among companies and their dynamic nature of relationships [6]. The problem is that there is a lack of more systematic and integrated methods to handle the several dimensions of risk, which includes both intra-organizational and inter-organizational aspects of the VO. Once the analysis of these risks is key to ensure the VO's proper operation, it should be complemented with the support of these methods, which can provide more agility and transparency in creating new VOs [7].

This paper presents an exploratory work, which complements the proposals of [2] and [7], and looks for answering how to properly analyse the risks in the VO formation process, given a set of pre-selected SPs. In this sense, this work increases the previous works by adding an additional risk management level in the SP's search and selection process through a new risk analysis method, named MARSP (Multi criteria Risk Analysis Method for selecting Service Providers in P2P SONs). In the proposed method, the SPs are two-stage evaluated, both individually and collectively. The goal of the method is to measure the level of risk and identify which SPs are most risky for the VO formation. This will allow decision-makers to decide wisely about which SPs should be effectively discarded for a given business collaboration opportunity, and additionally, the identified risks can be managed and hence mitigated throughout the VO formation process.

The remainder of this paper is organized as follows: Section II addresses the problem of SPs search and selection in P2P SONs and contextualizes it within the VO risk analysis proposal. Section III describes the proposed method for VO risk analysis. Section IV presents the preliminary experiments conducted to evaluate the proposed method. Finally, Section V concludes and discusses future directions.

II. General Background

A. Service Provider Integration

As cited in Section I, different SPs can be grouped in a given VO in order to accomplish a mutual goal, also referred to as collaboration opportunity. These SPs might range from non-governmental organizations to autonomous software entities, by sharing costs, benefits and risks, acting as they were one single enterprise [5]. The process of collaboration among SPs in a VO is accomplished by means of interactions between their business processes, which are usually supported by a network infrastructure. This work addresses the use of P2P SON to organize all the SPs committed with the eventual VO formation. A P2P SON is an infrastructure designed to

provide services and, in the context of this work, it can be seen as a breeding environment for the creation of VOs [8].

Regarding to the classical main phases of a VO life cycle (creation, operation, evolution and dissolution phases) [9], this paper focuses on the creation (or formation) phase, which is seen in Fig. 1. Within the creation phase, this analysis is carried out during the Partner's Search and Selection step (left circle), which was split in: the Best Peer Selection Service (BPSS) module [2] and the proposed risk analysis method (right circle). It is also considered that the SP's search and selection procedures are performed by a service management architecture developed in [10], and specifically through its BPSS module, which aims to select one SP from the set of found SPs that fulfil a required service according a particular metric.

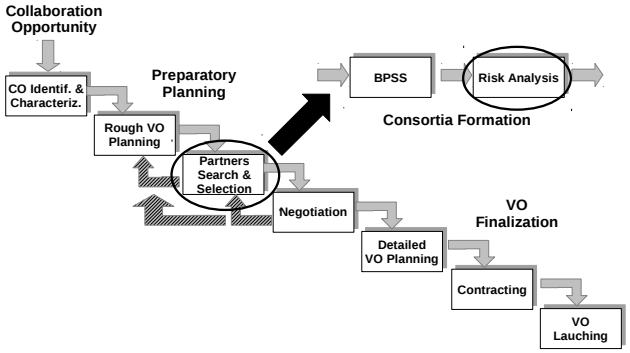

Fig. 1. Framework for the VO Formation Process. Extended from [9].

B. VO Formation Risk Analysis

The problem in choosing the most appropriate SPs to compose a VO is critical. The concept of risk can be handled at a number of perspectives [11], [12]. When applied on this research context, the risk can then be viewed as a composition of three basic elements: the general environment where it can happens; its occurrence probability; and the scope of its impact in the case of its occurrence [13].

In the state of the art review, some works related to risk analysis for VOs have been identified. In [6], [14], thirteen KPIs were identified as general risk sources in VOs, further identifying the importance of each one. In [15], the problem of risk mitigation in VO was discussed, and four processes were identified to improve the level of VOs performance reliability. In [16] two sources of risks were specified (external and internal), and risk occurrence likelihood in the life cycle of a VO was calculated based on them.

In spite of these reviewed works and the insights we have been taken from them, none have somehow formalized how the proposed KPIs should be used nor provided means to quantity VO partners risks before the VO formation. Moreover, it was not identified proposals that specify a method or procedure that aims to systematize the process of risk qualification/quantification involved in the SP's Search and Selection for the VO formation. Thus, this paper presents as a contribution a way to specify KPIs together with a mathematical method that enable measuring the risk in the VO formation.

C. Risk Sources Identification

The way the risk is represented should be aligned with the organization's goals so that the most important ones can be determined for further and more proper management [13]. Therefore, six main risks sources regarding VOs were identified, where three of them related to collaboration aspects and other three related to network infrastructure aspects. The collaboration risk sources are proposed by [6]:

- **Trust**: The degree of trust that exists between SPs is directly related to the amount of partners believe in honesty, generosity and overall competence of the others;
- **Communication**: Communication between the SPs in a VO is directly linked to the correct information about parts, products and services, collaborating in solving conflicts, sharing practices, among others;
- **Commitment**: Commitment is related to the attitude of VO members with each other, that is, it considers the contributions and agreements made by and among them for a business.

In addition to the risk sources related to collaboration aspects, there are the other three sources that concerns to infrastructre aspects proposed by [17]:

- **Distance:** represents the Euclidean distance between the requestor and the provider peer. It is based on the Internet delay model, which was built with real data [18].
- **Delay:** the time it takes to transmit a data packet from the source through routers and network links towards the destination;
- **Jitter:** statistical variation of the delay.

As a matter of quantification, the six previous risk sources will be seen in this work as KPIs, where three of them (trust, communication and commitment) defined under the term *Collaboration KPI* between SPs and three of them (distance, delay and jitter) defined under the term *Infrastructure KPIs*.

III. THE PROPOSED METHOD

In general, the main goal of the proposed risk analysis method is to add another support dimension for decision-making, identifying and measuring how risky is each of those SP candidates involved in the VO formation process. The devised method for risk analysis is presented in Fig. 2. The input of the proposed method is a list of pre-selected SPs (through BPSS simulation) in a P2P SON environment. The method splits the problem into two stages: the first phase does the individual risk analysis applying the Event Tree Analysis (ETA) [19] method. The second phase does the risk analysis taking the group of SPs as a whole into account, applying the Analytic Hierarchy Process (AHP) method [20].

1) Individual Risk Analysis: In the first phase, it is performed an individual risk analysis for the pre-selected SPs. ETA is particularly suitable for risk analysis of systems where there are interactions between several types of probabilistic events, whether dependent or independent [19]. It uses a visual representation based on a logical binary tree structure, known as Event Tree (ET), as shown in Stage 1 of Fig. 2.

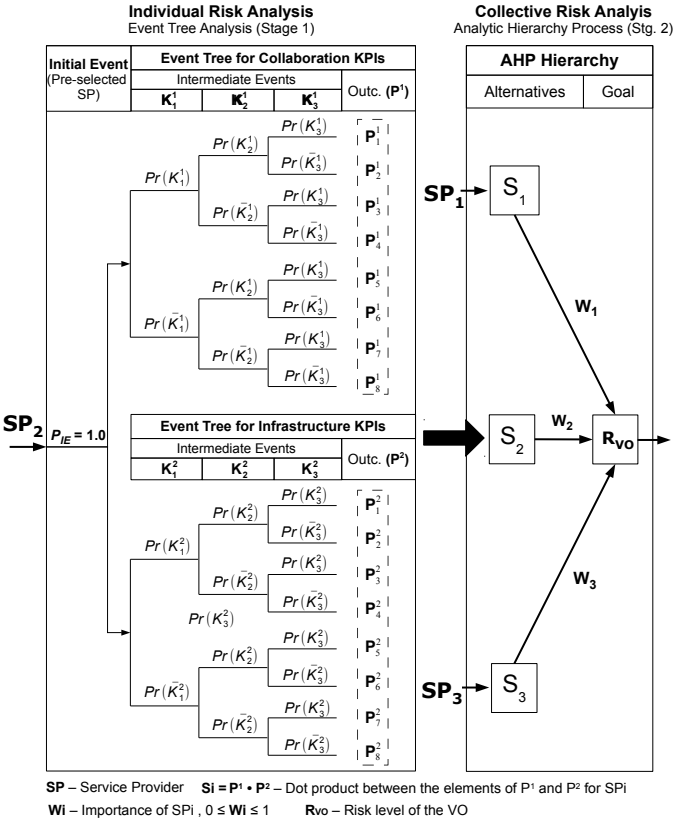

Fig. 2. MARSP Architecture.

An ET is a probability tree, which deals with two possible conditions: success and failure. It also has three basic components: initial event; intermediary events; and outcomes. The initial event begins the ET creation process. In this work, it corresponds to one pre-selected SP, and the assigned probability (P_{IE}) is always 1 (or 100%) in the beginning [19].

Next step consists of specifying the intermediary events for each of the two ETs that will be built. These events are represented by the two groups of (three) KPIs presented in Section II-C: *trust*, *communication* and *commitment* for the Collaboration ET; and *distance*, *delay* and *jitter* for the Infrastructure ET (Stage 1 of Fig. 2). They are used to quantify the risk of a particular SP on aspects of Collaboration and Infrastructure, and also to generate the two ETs by assigning success and failure probabilities for each them.

The criteria to assign the KPIs probabilities to each SP take the historical values analysis of the KPIs that were assigned to it in past VOs participations [21]. This analysis is fundamentally based on statistical inferences by quantifying both the central trend and variability of historical values. The central trend analysis is performed by calculating an exponentially weighted average index (EWA) [22] for each group G of historical KPI values of a given SP (where $G = 1$ for Collaboration KPIs; and $G = 2$ for Infrastructure KPIs).

The EWA is currently used in financial risk analysis and supply chain management being popular in practice due to its simplicity, computational efficiency and reasonable accuracy (giving more importance for the most recent values in an exponential factor) [22]. The EWA for a KPI k of a SP p is formally defined by Eq. 1:

$$\bar{X}_k^G(p) = \frac{\sum_{i=1}^{n} x_i w_i}{\sum_{i=1}^{n} w_i} \tag{1}$$

where $x = \{x_1, x_2, ..., x_n\}$ means a non-empty set of historical KPI values and w represents a normalized exponential decay constant. After calculating the EWA for each SP, the Maximum Quality Index (MQI) value is assigned as the higher value among all the results obtained with the EWA results of a given K_k^G for different SPs (that is, for $p = 1, 2, ...$). The MQI is calculated for each KPI and used as a performance reference for all others SPs that will be assessed. In this sense, considering k the number of used KPIs for each group (three) and p the number of SPs present in each of these two groups, Eq. 2 shows the MQI calculation procedure:

$$MQI_k^G = max_k\left(\bar{X}_k^G(p)\right) \quad \forall p \in SP \tag{2}$$

For instance, Fig. 3 shows a graph with hypothetical KPI values about *trust* (intermediate event KPI_1 of the Collaboration ET) associated to a SP. The value of the MQI assigned for this KPI was set up as 6.7 (this value is the highest EWA value calculated for all SPs using the KPI trust). Nevertheless, it is obvious that, when taking into account only the highest MQI, a few KPIs will reach an acceptable success probability. For this reason, a variability metric is welcome in this scope. The metric used is the standard deviation (SD) of MQI. Therefore, the acceptable interval will range not only values above 6.7, but also includes the SD interval, which are 2.4. So, the acceptable range turn to $6.7 - 2.4 = 4.3$.

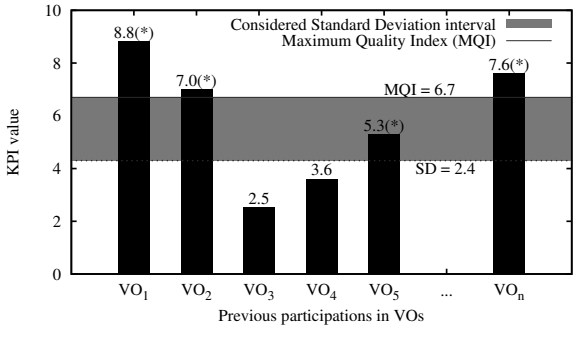

Fig. 3. Trust KPI historical values for a given SP.

The values assigned to each KPI of each group are normalized and can vary from 0 to 10, being associated

with a probability of success rate which varies from 0 to 1, respectively. Therefore, assuming that each SP has participated in n_{PA} past VOs and since that n_R represents the number of SP's previous participation in VOs where its KPIs values are higher than $MQI_k^G - SD_k^G$ (with an * in Fig. 3), Eq. 3 calculates the KPI success probability for the current participation.

$$Pr\left(K_k^G\right) = \frac{n_R}{n_{PA}} \tag{3}$$

The failure rate for a given KPI is represented as $Pr\left(\bar{K_k^G}\right)$ by the following equation:

$$Pr\left(\bar{K_k^G}\right) = 1 - Pr\left(K_k^G\right) \tag{4}$$

According to Fig. 2, the success and failure probability rates are calculated for all the two groups of KPIs that compose the Collaboration (at the top) and Infrastructure (at the bottom) ETs of a SP, which are presented by two groups of three intermediate (and independent from each other) events that populate each ET. Event K_2^1, for instance, would be related to KPI communication (Collaboration ET), with success and failure values of $P(K_2^1)$ and $1-P(K_2^1)$, respectively, while K_3^2 is related to KPI jitter (Infrastructure ET), with probabilities of success and failure of $P(K_3^2)$ and $1-P(K_3^2)$, respectively.

After assigning all probabilities for all two ETs branches, it is necessary to identify if the SPs are minimally qualified to compose a VO. For this, a calculation is performed to obtain the final probabilities for all event combinations composing the ETs. They are determined for each of the $2^{|K|}$ branches of each ET (number of elements in K) and are calculated by multiplying the probabilities of events that compose each path. Finally it is applied the dot product calculation in the set of results obtained in each of the two ETs, in order to obtain the level of risk for each SP.

The presented concepts can be formalized as follows:

Let $SP = \{SP_1, SP_2, ..., SP_n\}$ be a set of n SPs previously selected, where each element in this set is associated with a different type of service activity that is being requested in a business. For each SP_n, let $K^G = \left\{K_1^G, K_2^G, K_3^G\right\}$ a set of three KPIs, where for $G = 1$, it has been associated three Collaboration KPIs, and for $G = 2$ it has been associated three Infrastructure KPIs, and $Pr\left(K_k^G\right)$ the probability function associated with each event K_k^G (as defined in Eq. 3).

Now consider $P^G = \left\{P_1^G, P_2^G, ..., P_{|K|}^G\right\}$ as a set of all possible outcomes from the $2^{|K|}$ event combinations in each of the two ETs. The procedure for obtaining these sets was performed using a Binary Search Tree (BST), which travels $2^{|K|}$ different paths and assigns a value to each element of P^G, as shown in Eq. 5:

$$P^G = \bigcup_{k=1}^{2^{|K|}} \left[P_{IE} * \prod_{l=1}^{|K|} \omega(i,j,k,l) \right] \tag{5}$$

where P_{ie} is the initial probability of the SP. The function ω, as shown in Eq. 6, performs a binary search in the tree, returning a path element from each iteration. Values i and j correspond, respectively, to the beginning and ending of the search, and have $i = 0$ and $j = 2^{|K|}$ as initial values. The value k corresponds to the index of the sought element (an element of P^G) and l, the current level of the tree. The sequence of events can be viewed in Stage 1 of Fig. 2.

$$\omega\left(i,j,k,l\right) = \begin{cases} Pr\left(K_l^G\right); j = c, & k \leq c \\ 1 - Pr\left(K_l^G\right); i = c, & k > c \end{cases} \tag{6}$$

where $c = (i + j)/2$. After calculated the probabilities of all possible outputs P^G for a SP_n, it will be applied the dot product calculation over all the elements of P^1 and P^2, as formalized in Eq. 7. The use of the dot product as operation between the different P^G sets is justified by the possibility of simultaneous occurrences of two equals events, but in different ETs. For example, assuming that in Stage 1 of Fig. 2, $P_1^1 = 0.7$ (Collaboration ET), which represents a probability of 70% chance of the combination of three events (success for K_1^1, K_2^1 and K_3^1) occur. Similarly, if $P_1^2 = 0.8$ (Infrastructure ET), it means that the same sequence of events (success for K_1^2, K_2^2 and K_3^2) also occurred. Thus, using the dot product between the (two) values P^1 and P^2, it can be obtained the final risk level of the SP_n (which is represented by S_n):

$$S_n = P^1 \cdot P^2 = \sum_{i=1}^{2^{|K|}} P_i^1 P_i^2 \tag{7}$$

The final probability values obtained by Eq. 7 will be used to measure and analyze the SP's risk collectively.

2) Collective Risk Analysis: The second phase of the MARSP method aggregates the results provided by the first phase (that is, the risk level of each pre-selected SPs) to calculate the VO success probability as a whole (if the VO formation can succeed or not). To perform this, it is used the Analytic Hierarchy Process (AHP) [20], as seen in Stage 2 of Fig. 2. In AHP, the problems are arranged in a hierarchy, starting from the more general element (usually the goal) to the most specific elements (often alternatives). In this paper, the AHP is specified by two components: the goal and the alternatives. The goal of AHP is to determine the overall VO risk. The alternatives consist in the individual risk levels for each SP (S_n) obtained through the individual risk analysis (Stage 1 of Fig. 2).

For each alternative S_i there is also a correspondent weight w_i, which determines the degree of importance of each SP_i regarding the VO. In this work, the degree of importance of each SP is determined by an external entity named VO Manager [5], which is seen as the main decision maker. Therefore, the VO Manager plays a key function in the process of evaluating the VOs since he will inform which SPs have greater or lesser importance, so prioritizing some specific SPs in relation to the other ones.

For example, given a VO in the formation process, composed by three SPs (as illustrated in Fig. 2), each SP will have a level of importance (weight). In this sense, the

VO Manager can change the weights w_i according to the degree of importance that is assigned to each SP_i. This feature increase the robustness of the method when compared to other techniques, by determining collectively the influence that each SP has within the VO and the level of risk of each one will impact the level of overall risk of VO.

Accordingly, let $W_1, W_2, ..., W_n$ is the weight of each alternative $S_1, S_2, ..., S_n$ associated the goal. The overall goal (measure the risk level of the VO) is represented by R_{VO} whose simplified calculation procedure is shown in Eq. 8:

$$R_{VO} = 1 - \sum_{i=1}^{n} W_i S_i \quad (8)$$

From the calculation presented in Eq. 8, is obtained the overall level of risk in the VO formation, considering the importance of each SP in the process.

IV. Evaluation

A. Computational Prototype

The developed prototype was split into two modules: BPSS (Best Peer Selection Service) and DFRA (Decision Framework for Risk Analysis). The first module implements the BPSS model developed by [2] (view Section II-A) by using the PeerFactSim.KOM discrete event simulator [23] to make available the process for SPs search and selection. On the other hand, the DFRA module focuses specifically on the risk analysis methods simulation. This model was integrated with BPSS in order to group the pre-selected SPs into a new potential VOs and to perform a MARSP evaluation.

B. Simulations Setup

The data (set of SPs) was taken from the CAIDA project and MaxMind GeoIP database [18], which also provide the geographic position and delay of each SP. From these metrics, the values of the Infrastructure KPIs (bandwidth, jitter and Euclidean distance) are calculated. The values of the Collaboration KPIs assigned for each SP follow a linear distribution (varying from 0 to 1 with intervals of 0.01) during the simulation, due to the difficult to measure them in real scenarios. It is also considered that each SP has participated at 10 previous VOs (in average) when it was selected.

For the sake of simplicity, the importance of each SP in a VO is equally established. The range of values that determines the risk level of a VO (100 possible values) is generalized by the following evaluation scores [16]: $[0.0; 0.25]$: very low (L_1); $[0.25; 0.50]$: relatively low (L_2); $[0.50; 0.75]$: relatively high (L_3); $[0.75; 1.00]$: very high (L_4).

C. Results

The results presented in this section aim to evaluate the categorized level of risk in the formation of VOs, given a set of previously selected SPs. Due to the originality of the proposed method, that is, given the lack of methods in the literature that enables an efficient comparative analysis, it was sought to direct the analysis of the results regarding the performance aspects of the method. Specifically, this work explores its scalability, which is related to the variation in the number of SPs that will compose a VO. The procedures for evaluating these VOs are mainly divided into two phases: 1) performs the process of SP's search and selection through the BPSS model; and 2) using as input the pre-selected SPs to group them into a consortia and measure (through Collaboration and Infrastructure KPIs) the category of risk of their collaboration in composing a new VO.

The results comprise six different scenarios, where each one represents a set of simulations for VOs formed by $3, 4, ..., 8$ SPs. Fig. 4 presents the results of simulations, showing, for each scenario:

- The amount of VOs (in %) who achieved level risk associated with each rating category (L_1, L_2, L_3 and L_4 respectively). These results are represented by the 4-bar cluster in Fig. 4 and related with the left vertical axis;
- The average of the absolute risk values of all simulated VOs (in %). These results are represented by the line in Fig. 4 and are related with the right vertical axis. In addiction, the standard deviation is calculated for each scenario, basing in a confidence interval of 95%.

Specifically, each scenario includes the simulation of 100 formed VOs from a database of 300 SPs in a P2P SON. Therefore, it was performed 100 times the two aforementioned phases (where each simulation was repeated 10 times to obtain average results), resulting in 100 possible VOs to be analyzed for each scenario.

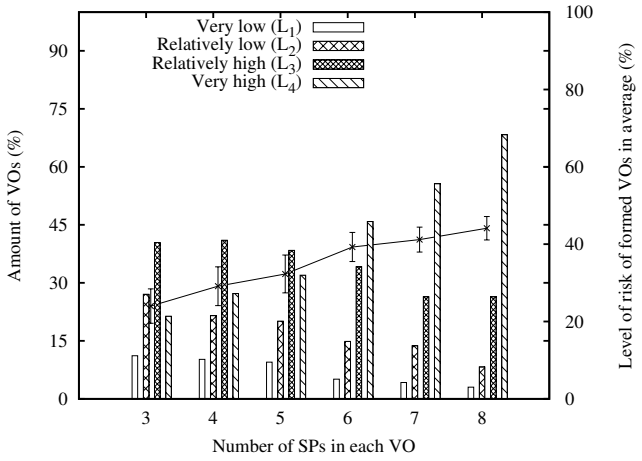

Fig. 4. Distribution of the risk classifications and average simulations involving six different scenarios for the formation of VOs

From the results shown in Fig. 4, one can see that most of the evaluated scenarios presented a very high (L_4) or relatively high (L_3) level of risk in forming VOs. Moreover, the amount of VOs in these two categories were enhanced when there is an increase in the number of SPs for each VO. The high risk classification (L_3 and L_4) that appears in all scenarios reflects some aspects that regard to the individual performance of each SP, that is, a SP can have good classification of its Infrastructure KPIs, but lack the collaboration necessary to ensure good performance of the VO

and vice versa. Since this factor is very important in deciding the individual risk classifications of the SPs, it consequently affect the performance of the VO as a whole.

Regarding the average level of risk for each scenario (line in Fig. 4), one can note that there is a increase in its value when increased the number of SPs in VOs. It occurs because the more SPs are being analyzed, the greater becomes the probability that the previously selected SPs have KPIs with values on many different levels. As the risk analysis carried out by the proposed method bases on the average presented by the SP with have the greater KPI values (MQI – Section III), the presence of SPs with low KPI values increases the likelihood of differences between KPI values, thus increasing the level of risk as a whole.

In this sense, it can be concluded that the method favours a more rigorous evaluation when is encompassed an increased number of SPs per VO, and therefore should be taken into account a greater prevention and control of risk in order to provide greater security in a future operation of the VO. Moreover, for all SPs that will compose a VO, it is necessary that all their KPIs (Collaboration and Infrastructure) have reasonably acceptable values. Otherwise, they can compromise the proper working of the VO.

V. Conclusion

This paper presented an exploratory work that addresses some issues related to VO risk identification and measurement. Overall, risk analysis has become a key element in VO planning since small errors can lead them to impairment as a whole. For this reason, it is proposed a new method to perform a risk analysis in a set of Service Providers (SPs) that are going to compose a Virtual Organization (VO). The presented method, named MARSP, is composed of two stages. The first stage performs an individual risk analysis for all pre-selected SPs, by basing it on ETA analysis. Having as input the results from the first stage, the second stage calculates and analyses the global risk considering all SPs together. It applies the AHP method to accomplish that.

In order to assess the MARSP behaviour, there was performed a simulation that involved sets of pre-selected SPs, which have been taken in [2]. The assessments explored the performance of the method regarding its scalability, that is, evaluating how the method behaves in accordance with an increasing number of SPs composing a VO. The level of effectiveness required for each SP to compose a VO is higher and it is strongly influenced by both aspects of collaboration and network infrastructure in which the SPs are inserted. Therefore, to effectively form a VO, it should be aligned a strict amount of SPs that have strong collaborative ties, together with quality of the network service.

Likewise, the presented method contributes to a more concrete way to express, measure, assess and deal with the risks in VO formation, both individually and collectively, while focusing only on SPs. Nevertheless, the use of the method in the process of risk analysis provides an evaluation with a lower level of subjectivity, discarding SPs or not, before composing a VO, according to the established criteria. The next steps from the results obtained in this work includes testing the method in near-real scenarios as well as well as the comparison with other decision support methods.

References

[1] Z. Duan, Z. L. Zhang, and Y. T. Hou, "Service overlay networks: SLAs, QoS, and bandwidth provisioning," *IEEE/ACM Transactions on Networking*, vol. 11, no. 6, pp. 870–883, 2003.

[2] A. Fiorese, P. Simões, and F. Boavida, "Peer selection in P2P service overlays using geographical location criteria," in *12th Int. Conf. on Computational Science and Its Applications*, Salvador de Bahia, Brazil, 2012, pp. 234–248.

[3] S. Zhou, M. Hogan, S. Ardon, M. Portman, T. Hu, K. Wongrujira, and A. Seneviratne, "Alasa: When service overlay networks meet peer-to-peer networks," in *11th Asia-Pacific Conf. on Communications*, Perth, Australia, 2005, pp. 1053–1057.

[4] A. Mowshowitz, "Virtual organization," *Communications of the ACM*, vol. 40, no. 9, pp. 30–37, 1997.

[5] L. M. Camarinha-Matos and H. Afsarmanesh, "On reference models for collaborative networked organizations," *Int. J. of Production Research*, vol. 46, no. 9, pp. 2453–2469, 2008.

[6] M. Alawamleh and K. Popplewell, "Risk sources identification in virtual organisation," in *Enterprise Interoperability IV*. Springer London, 2010, pp. 265–277.

[7] O. C. A. Junior and R. J. Rabelo, "A KPI model for logistics partners' search and suggestion to create virtual organisations," *Int. J. of Networking and Virtual Organisations*, vol. 12, no. 2, pp. 149–177, 2013.

[8] H. Afsarmanesh and L. M. Camarinha-Matos, "A framework for management of virtual organization breeding environments," in *6th Work. Conf. on Virtual Enterprises (PRO-VE'05)*, Valencia, Spain, 2005, pp. 35–48.

[9] L. M. Camarinha-Matos and H. Afsarmanesh, "Collaborative networks: a new scientific discipline," *Journal of Intelligent Manufacturing*, vol. 16, no. 4-5, pp. 439–452, 2005.

[10] A. Fiorese, P. Simões, and F. Boavida, "OMAN – a management architecture for P2P service overlay networks," in *4th Int. Conf. on Autonomous infrastructure, management and security*, Zurich, Switzerland, 2010, pp. 14–25.

[11] J. G. March and Z. Shapira, "Managerial perspectives on risk and risk taking," *Management Science*, vol. 33, no. 11, pp. 1404–1418, 1987.

[12] H. Moskowitz and D. Bunn, "Decision and risk analysis," *European Journal of Operational Research*, vol. 28, no. 3, pp. 247–260, 1987.

[13] D. Vose, *Risk analysis: a quantitative guide*. New Jersey, USA: Wiley & Sons, 2008.

[14] M. Alawamleh and K. Popplewell, "Analysing virtual organisation risk sources: an analytical network process approach," *Int. J. of Networking and Virtual Organisations*, vol. 10, no. 1, pp. 18–39, 2012.

[15] M. Grabowski and K. H. Roberts, "Risk mitigation in virtual organizations," *Journal of Computer-Mediated Communication*, vol. 3, no. 4, pp. 704–721, 1998.

[16] Y. Li and X. Liao, "Decision support for risk analysis on dynamic alliance," *Decision Support Systems*, vol. 42, no. 4, pp. 2043–2059, 2007.

[17] A. Fiorese, F. Matos, O. C. A. Junior, and R. M. Ruppenthal, "Multi-criteria approach to select service providers in collaborative/competitive multi-provider environments," *Int. J. of Computer Science and Network Security*, vol. 13, no. 9, pp. 15–22, 2013.

[18] Caida, "Macroscopic topology project," 2013, http://www.caida.org/analysis/ topology/macroscopic/.

[19] C. A. Ericson, *Hazard analysis techniques for system safety*. New York, USA: Wiley & Sons, 2005.

[20] T. L. Saaty, "Decision making – the analytic hierarchy and network processes (ahp/anp)," *Journal of Systems Science and Systems Engineering*, vol. 13, no. 1, pp. 1–35, 2004.

[21] H. T. Goranson, *The agile virtual enterprise cases, metrics, tools*. Westport, CT, USA: Quorum Books, 1999.

[22] D. C. Montgomery and G. C. Runger, *Applied Statistics and Probability for Engineers*. New Jersey, USA: Wiley & Sons, 2011.

[23] D. Stingl, C. Gross, J. Ruckert, L. Nobach, A. Kovacevic, and R. Steinmetz, "PeerfactSim.KOM: a simulation framework for peer-to-peer systems," in *13th Int. Conf. on High Performance Computing and Simulation*, Istanbul, Turkey, 2011, pp. 577–584.