

Análise de Risco em Redes P2P baseada em KPIs de Colaboração e de Infraestrutura

Rafael Giordano Vieira¹, Omir Correia Alves Junior¹ and Adriano Fiorese¹

¹Departamento de Ciência da Computação
Universidade do Estado de Santa Catarina (UDESC) – Joinville – SC – Brazil

{rafaelgiordano12, omalves, adriano.fiorese}@gmail.com

Abstract. *The development of collaborative networked 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 sense, this paper presents a supporting decision method for selecting the most suitable SPs within a P2P network, taking into account a risk analysis 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.*

Resumo. *O desenvolvimento de ambientes colaborativos em rede tornou-se um fator chave para que Provedores de Serviços (PSs) possam alavancar com sucesso suas atividades de mercado. No entanto, a volatilidade dessas redes propicia diversos riscos adicionais, que precisam ser identificados, medidos e mitigados através de um processo bem definido. Nesse sentido, este artigo apresenta um método de apoio à tomada de decisão que realiza a seleção de PSs em redes P2P, levando em conta uma análise de risco baseada em KPIs de colaboração e de infraestrutura de redes para a composição de Organizações Virtuais (OVs). Um protótipo computacional também foi desenvolvido para executar um conjunto de simulações de modo a avaliar a eficiência do método proposto.*

1. Introdução

Nos últimos anos, a prestação de serviços tornou-se uma das principais fontes de receitas em toda a Internet. Em particular, a evolução das Redes de Sobreposição de Serviços P2P (P2P SON) [Duan et al. 2003, Fiorese et al. 2012] têm proporcionado um ambiente favorável para que os Provedores de Serviços (PSs) possam tornar os seus serviços disponíveis à comunidade de usuários em geral. A combinação das redes P2P e SON oferece um elevado potencial para o gerenciamento de serviços, impulsionada pela criação de redes dinâmicas e auto-organizáveis entre os diversos PSs. Além disso, uma grande variedade de serviços pode ser disponibilizada nessas redes, onde preço e qualidade podem ser diferenciais competitivos [Zhou et al. 2005].

O conceito de P2P SON se aplica a uma ampla gama de aplicações de rede. Este artigo lida particularmente com um tipo de aplicação de rede específico, denominada Organização Virtual (OV). Uma OV pode ser entendida como uma aliança estratégica dinâmica e temporária, formada por empresas autônomas, heterogêneas e, geralmente,

geograficamente dispersas, criadas para atender uma oportunidade de negócio específica [Mowshowitz 1997, Camarinha-Matos and Afsarmanesh 2008]. Neste sentido, uma P2P SON proporciona um ambiente para a formação das OVs e ao mesmo tempo fornece benefícios para os PSs que a compõe, ou seja, proporciona a partilha de custos, largura de banda, dentre outros [Fiorese et al. 2010].

Embora as vantagens proporcionadas pela utilização de P2P SONs possam melhorar o processo de formação de uma OV, a grande volatilidade presente na estrutura de uma OV implica em alguns riscos adicionais, que possuem fontes incertas quando comparadas a estilos tradicionais de cooperação [Alawamleh and Popplewell 2010]. Por esta razão, a formação de uma OV não é garantida e necessita do apoio de métodos que quantifiquem o risco envolvido e para tanto necessitam de um ou mais critérios para análise, apoiado por um conjunto de indicadores de desempenho chave (KPIs) [Junior and Rabelo 2013]. A utilização desses métodos, além de propiciar menor nível de subjetividade na análise, se mostram adequados especialmente quando se trata de redes de serviços mais complexas [Neely et al. 1997].

Em um trabalho anterior, os mesmos autores projetaram uma arquitetura de três camadas para o gerenciamento de serviços em P2P SONs, chamada OMAN [Fiorese et al. 2010]. A OMAN provê um mecanismo eficiente para a busca e seleção dos PSs mais adequados em um ambiente com múltiplos PSs. No entanto, os aspectos de risco em OVs no contexto das redes P2P SON não foram abordados.

Este artigo apresenta um trabalho de pesquisa exploratória que complementa os trabalhos de [Fiorese et al. 2012] e [Junior and Rabelo 2013] e tem como objetivo responder como os PSs podem ser selecionados adequadamente ao serem considerados os riscos no processo. Nesse sentido, este trabalho consiste na adição de uma camada adicional com o objetivo de realizar o gerenciamento de riscos no processo de busca e seleção de PSs, através da criação de um método de análise de risco chamado MAR-SP (*Multicriteria Risk Analysis method for selecting Service Providers in P2P SONs*). No método proposto, os PSs são avaliados em duas etapas, tanto individualmente como coletivamente. O objetivo do método é medir o nível de risco através de KPIs de colaboração e de infraestrutura em P2P SONs, a fim de identificar quais os PSs oferecem menor nível de risco para a formação de uma nova OV. Isto irá permitir que os tomadores de decisão possam decidir com um nível muito menor de subjetividade sobre quais PSs devem ser descartados de forma eficaz para uma determinada oportunidade de colaboração.

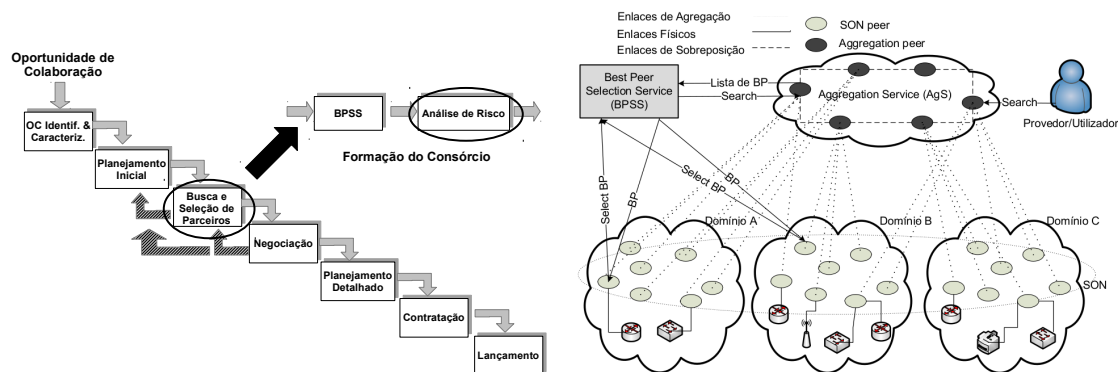
As demais seções deste artigo estão organizadas da seguinte forma: a Seção 2 aborda o problema da integração e seleção dos PSs no contexto de análise de risco em OVs. A Seção 3 descreve o método proposto para análise de risco em OVs. A Seção 4 apresenta os experimentos realizados para avaliar o método proposto e também apresenta resultados preliminares. Finalmente, a Seção 5 conclui e discute trabalhos futuros.

2. Trabalhos Relacionados

2.1. Integração de Provedores de Serviços

Como citado na Seção 1, diferentes PSs podem ser integrados em uma OV e colaborar entre si a fim de atender a uma Oportunidade de Colaboração (OC). Esses PSs podem compreender desde organizações não governamentais até entidades de software

autônomas, possuindo diferentes objetivos, mas que compartilham competências, recursos, informações e eventuais riscos, permitindo-lhes realizar seus objetivos comuns. O ciclo de vida de uma OV é composto por quatro fases (criação, operação, evolução e dissolução) [Camarinha-Matos and Afsarmanesh 2005], sendo que este trabalho se concentra na fase de criação. A fase de criação de uma OV é composta por sete etapas, como pode ser visualizado na Figura 1(a). Nesse sentido, esse trabalho insere-se na etapa de Busca e Seleção de Parceiros (círculo à esquerda da Figura 1(a)).



(a) Etapas para a criação de uma OV. Adaptado de [Camarinha-Matos and Afsarmanesh 2005]

(b) Modelo BPSS [Fiorese et al. 2012]

Figura 1. Visão geral do contexto do trabalho

O processo de colaboração entre os PSs em uma OV é realizado por meio de interações entre seus processos de negócio, que são usualmente suportados por uma infraestrutura de rede. Esta pesquisa aborda a utilização de P2P SONs como infraestrutura para suportar a criação de uma OV. Considera-se também que os procedimentos para a busca e seleção dos PSs para compor uma OV é realizada pela arquitetura de gerenciamento de serviços (desenvolvida pelos mesmos autores) chamada OMAN [Fiorese et al. 2010], dando ênfase particular na sua terceira camada, que é responsável por realizar a seleção dos PSs mais adequados na P2P SON.

A Figura 1(b) apresenta o modelo do BPSS. Ele está dividido em três partes. Os pares SON (definidos como círculos cinza claros) representam essencialmente os PSs que podem oferecer/publicar um serviço ou um componente de serviço. Os pares de agregação (círculos cinza escuros) correspondem aos PSs que formam uma segunda sobreposição, denominada AgS (*Aggregation Service*), para agrupar um conjunto de serviços oferecidos pelos pares SON. Finalmente, o serviço de seleção do melhor par (BPSS) (quadrado cinza) em si é um mecanismo que seleciona um PS específico entre todos os encontrados através de uma pesquisa iniciada por um determinado par SON (definido como o provedor/usuário) [Fiorese et al. 2012]. As linhas tracejadas representam a comunicação entre os pares SON e AgS e as linhas contínuas representam as interações de busca e seleção do melhor PS.

O modelo BPSS tem como principal objetivo selecionar um PS a partir do conjunto de PSs encontrados que fornecem o serviço requerido de acordo com um indicador de desempenho específico. No modelo atual empregado por [Fiorese et al. 2012], os PSs são selecionados baseados na métrica de Distância Euclidiana [Kaune et al. 2009]. O método proposto para a análise de risco utiliza o módulo BPSS a fim de obter um con-

junto de PSs (um para cada serviço), quando considerando os diferentes tipos de serviços necessários para compor uma OV.

2.2. Risco em Organizações Virtuais

O problema na escolha dos PSs mais adequados para compor uma OV é crucial. O ambiente em que os PSs realizam suas atividades é caracterizado por uma série de fontes de risco, podendo ser elas provenientes de origem econômica, social, política, como também riscos na própria infraestrutura da rede. O conceito de risco pode ser apresentado através de diferentes perspectivas. [March and Shapira 1987] define o risco como a variação na distribuição dos possíveis resultados, as suas probabilidades, e seus valores subjetivos. [Mowshowitz 1997] refere-se ao risco como sendo um conjunto de probabilidades associadas às alternativas de decisão com resultados incertos, sendo estes favoráveis ou desfavoráveis. Quando aplicado no contexto desta pesquisa, o risco pode ser visto como uma composição de três elementos básicos: o ambiente onde ele pode acontecer, a sua probabilidade de ocorrência, e o âmbito do seu impacto no caso da sua ocorrência [Vose 2008].

Na literatura, alguns trabalhos relacionados à análise de risco em OVs foram identificados. Em [Alawamleh and Popplewell 2012, Alawamleh and Popplewell 2010], treze indicadores foram identificados como potenciais fontes de risco em OVs, sendo identificada a importância de cada um deles. Em [Li and Liao 2007] foram especificadas duas fontes de risco (externo e interno) e a probabilidade de ocorrência de riscos no ciclo de vida da OV foi calculado com base nelas. Em [Grabowski and Roberts 1998], foi discutido o problema da mitigação do risco em OVs, e quatro processos foram identificados para melhorar o seu nível de confiabilidade. No entanto, na pesquisa bibliográfica que foi realizada, não identificou-se propostas que especificam um método ou procedimento que tenha como objetivo sistematizar o processo de qualificação e quantificação do risco envolvido na busca e seleção de PSs para a formação de uma OV.

Nesse sentido, o processo para a criação de uma OV apresentado na Figura 1(a) foi estendido pela adição de algumas sub-etapas na etapa de Busca e Seleção de Parceiros. Em primeiro lugar, o modelo BPSS (como visto na Seção 2.1) é utilizado para fornecer um ambiente para a busca e seleção dos PSs. Em seguida, é adicionado um processo que compreende a análise de risco (círculo direita na Figura 1(a)). Nesse caso, dada uma OV em formação (composta por PSs), um conjunto de indicadores de desempenho adequados são inicialmente selecionados, e a seleção final irá considerar a perspectiva de risco.

A forma como o risco é representado deve estar estritamente alinhado com os objetivos de cada organização. Identificar as fontes de risco é o primeiro e mais importante passo na gestão de riscos [Vose 2008]. Portanto, através da pesquisa bibliográfica realizada identificou-se seis fontes de risco que estão associadas às OVs e que foram propostas por [Alawamleh and Popplewell 2010] e [Fiorese et al. 2013]. Estas fontes de risco são referentes aos aspectos de *colaboração* entre os PSs e de aspectos relacionados à *infra-estrutura* das redes P2P. As fontes de riscos quando relacionadas à colaboração são: a *confiança*, a *comunicação* e o *comprometimento* [Alawamleh and Popplewell 2010]:

- **Confiança:** Os PSs que vão compor uma OV não necessariamente precisam possuir conhecimento prévio sobre os outros antes de iniciar a colaborar. Assim, a confiança torna-se um aspecto fundamental, que por sua vez envolve compromisso

em realizar as tarefas planejadas. Quando a confiança entre os PSs não é suficientemente estabelecida, há uma hesitação para compartilhar riscos e por isso a OV pode ser comprometida;

- **Comunicação:** A comunicação entre os PSs de uma OV é um fator fundamental para o seu funcionamento adequado. Eles devem fornecer informações corretas sobre produtos e serviços, colaborando na solução de conflitos, riscos, etc. No entanto, isso pode ser complicado pelo fato de os PSs serem heterogêneos, independentes, geograficamente dispersos, e geralmente possuem culturas de trabalho distintas. A falta de comunicação pode colocar assim uma OV em risco;
- **Comprometimento:** O comprometimento está diretamente relacionado com as atitudes dos PSs uns com os outros em uma OV, ou seja, considera as contribuições e os acordos feitos por e entre eles para um negócio. O risco da OV fica maior quando os PSs falham nessa atitude.

Além das fontes de risco relacionadas aos aspectos de colaboração, é necessário levar em conta que, devido ao fato de o processo para a busca e seleção ser destinado a PSs que oferecem, na maioria, serviços de rede (principalmente na Internet), os indicadores de risco utilizados neste trabalho também devem levar em conta critérios que fornecem garantias de QoS (Qualidade de Serviço) para todos os outros PSs que irão compor a OV (indicadores de infraestrutura aplicado a redes P2P). Por esta razão, os seguintes indicadores foram escolhidos [Fiorese et al. 2013]:

- **Distância:** Representa a distância Euclidiana entre os PSs. Ela baseia-se no modelo de atraso de Internet [Kaune et al. 2009] (*delay* na troca de mensagens), onde os PSs são colocados em um plano cartesiano, utilizando métricas de desempenho de rede, juntamente com as suas coordenadas geográficas para analisar a distância entre eles. Uma distância elevada pode acarretar em atraso na entrega de pacotes, maior custo, dentre outros.
- **Atraso:** Consiste no tempo que um pacote leva para sair da sua origem, passar por uma rede (roteadores e enlaces) e chegar ao destino. O atraso é dado pela soma dos tempos de processamento, atraso de fila, de transmissão e o de propagação.
- **Jitter:** O *jitter* é a variação estatística do atraso na entrega de dados. Os pacotes são enviados uniformemente na rede, porém os mesmos não chegam aos seus destinos nos mesmos intervalos, devido aos diversos fatores que influenciam no atraso de um pacote, como por exemplo, a diferença de tempo de processamento dos pacotes, tempo de acesso à rede e de enfileiramento.

Por uma questão de quantificação, as seis fontes de risco especificadas nesse trabalho serão vistas como KPIs, sendo três delas (confiança, comunicação e comprometimento) definidas sob o termo de KPIs de Colaboração entre os PSs e outras três delas (distância, atraso e *jitter*) definidas sob o termo KPIs de Infraestrutura para redes P2P.

3. Método Proposto

O método concebido para a análise de risco é apresentado na Figura 2. Ele começa tendo como entrada uma lista ordenada com os PSs pré-selecionados mais adequados (por meio da simulação BPSS) registrados em um ambiente P2P SON. O principal objetivo do método de análise de risco proposto é acrescentar uma outra dimensão de apoio

para a tomada de decisões, identificar e medir o quão arriscado é cada um desses candidatos (PSs) envolvidos na formação de uma nova OV. O método divide o problema em dois estágios: o primeiro estágio consiste na análise de risco individual através aplicação do método ETA (*Event Tree Analysis*) [Ericson 2005, Vose 2008] para cada grupo de KPIs (Colaboração e Infraestrutura). O segundo estágio realiza a análise de risco levando em conta um conjunto de PSs como um todo, através da aplicação do método AHP (*Analytic Hierarchy Process*) [Saaty 1996, Saaty 2004].

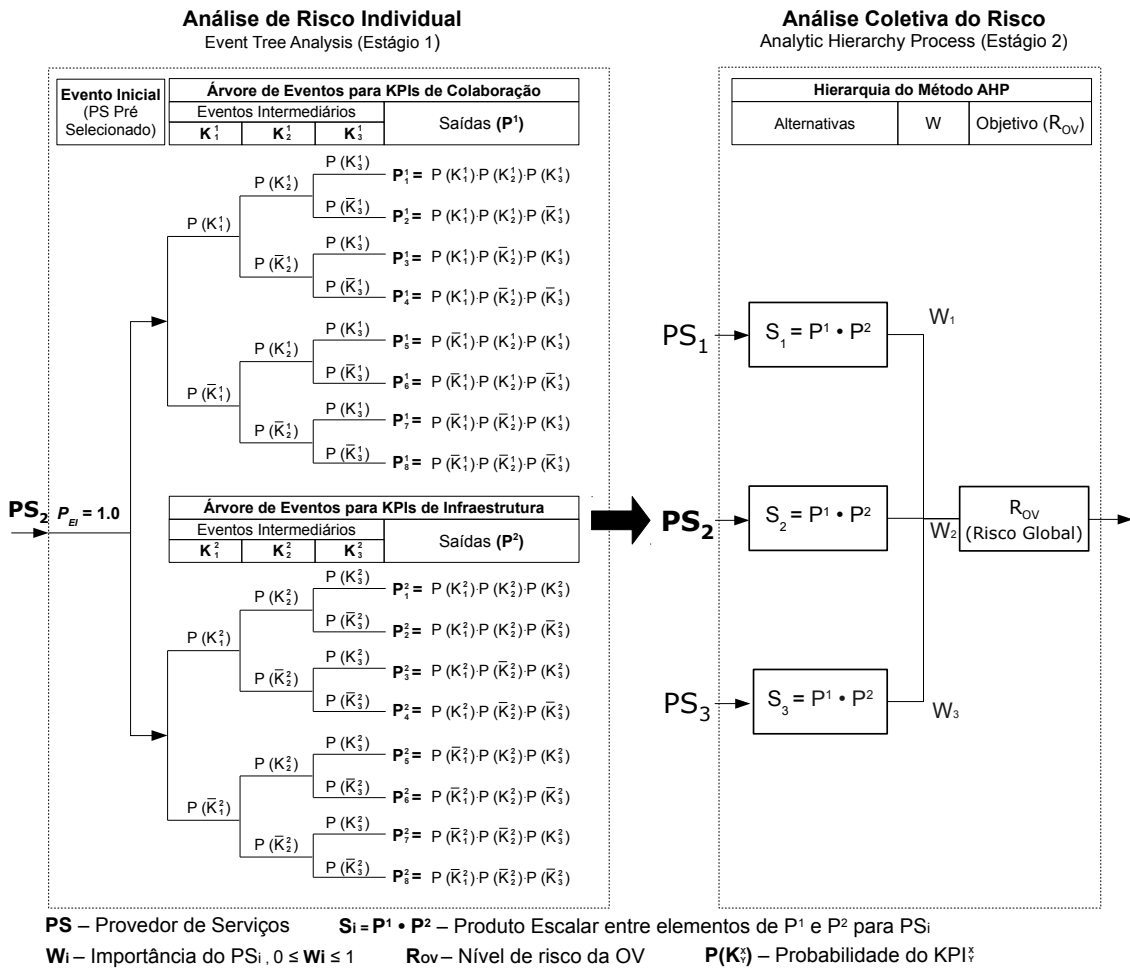


Figura 2. Visão geral do método MAR-SP.

3.1. Análise de Risco Individual

No primeiro estágio do método MAR-SP é realizada a análise de risco individual para cada PS pré-seleccionado (através do BSS). O método ETA é particularmente adequado para a análise de risco de sistemas em que existam interações entre os vários tipos de eventos probabilísticos, sejam eles dependentes ou independentes [Ericson 2005]. Ela utiliza uma representação visual baseada em uma estrutura lógica em forma de árvore, conhecida como árvore de eventos (ET), como mostrada no Estágio 1 da Figura 2.

Uma ET consiste em uma árvore de probabilidades (binária) que admite duas possíveis condições: sucesso e fracasso. Ela possui três componentes básicos, que são:

evento inicial (EI); eventos intermediários; e os possíveis resultados. O evento inicial corresponde ao evento que dá início ao processo de formação da ET. Nesse trabalho, o EI corresponde à pré-seleção de um PS e a probabilidade associada a esse evento (P_{EI}) é sempre igual a 1 (ou 100 %) [Ericson 2005].

O próximo passo consiste em especificar os eventos intermediários para cada uma das duas ETs que serão construídas, onde esses eventos são representados pelos dois grupos de (três) KPIs apresentados na Seção 2: *confiança, comunicação e comprometimento* para a ET de Colaboração; e *distância, atraso e jitter* para a ET de Infraestrutura (Estágio 1 da Figura 2). Estes eventos são utilizados para quantificar a eficácia de um determinado PS sob ambos os aspectos de colaboração e de infraestrutura e também para gerar as duas ETs, atribuindo probabilidades de sucesso e falha a cada uma delas.

O critério para atribuir a probabilidade de sucesso dos KPIs para cada PS leva em conta a análise histórica de valores dos KPIs que foram atribuídos ao PS nas últimas participações em OV's [Pidduck 2006, Goranson 1999]. Essa análise baseia-se fundamentalmente em inferências estatísticas por meio da quantificação tanto de uma tendência central quanto da variabilidade dos valores históricos. A análise de tendência central é realizada através do cálculo de uma média exponencialmente ponderada (MEP) [Montgomery and Runger 2011] para cada grupo G de valores históricos de KPIs de um determinado PS ($G = 1$ para KPIs de Colaboração; $G = 2$ para KPIs de Infraestrutura).

A MEP é muito utilizada em análise de risco financeiro e de gestão da cadeia de suprimentos, sendo popular na prática devido à sua simplicidade, eficiência computacional e precisão razoável (dando mais importância para os valores mais recentes em um fator exponencial) [Montgomery and Runger 2011]. A MEP para um KPI k de um PS p é formalmente definida pela Equação 1:

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

onde $x = \{x_1, x_2, \dots, x_n\}$ corresponde a um conjunto não vazio com n valores históricos de KPIs e w representa uma constante de decaimento exponencial normalizada. Após calcular a MEP para cada KPI de cada PS, é definido um valor denominado Índice Máximo de Qualidade (IMQ), que é atribuído como o valor mais alto entre todos os resultados obtidos com a MEP de um determinado K_k^G para diferentes PSs (ou seja, para $p = 1, 2, \dots$). O IMQ é usado como uma referência de desempenho (limiar) para todos os outros PSs que serão avaliados. Neste sentido, considerando k o número de KPI utilizados em cada grupo (três) e p o número de PSs associados aos dois grupos de KPIs, a Equação 2 define o processo de cálculo do IMQ:

$$IMQ_k^G = \max_k (\bar{X}_k^G(p)) \quad \forall p \in PS \quad (2)$$

Por exemplo, as Figuras 3(a) e 3(b) apresentam dois gráficos com os valores hipotéticos dos KPIs de *confiança* (evento intermediário K_1^1 na ET de Colaboração) e *distância* (evento intermediário K_1^2 na ET de Infraestrutura) associado a um PS. Tomando como exemplo a Figura 3(a), o valor do IMQ calculado para este KPI é de 6.7 (dentro todos as MEPs calculadas para este KPI, este valor é o valor mais alto). No entanto,

é evidente que, quando se leva em conta apenas o valor do IMQ, ou seja, a MEP mais elevada, apenas alguns valores de KPIs da série história dos demais PSs atingirão uma probabilidade de sucesso aceitável. Por esta razão, uma métrica de variabilidade torna-se bem adequada, sendo representada pelo desvio-padrão (DP) do IMQ. Portanto, serão considerados para análise, além dos valores acima de 6.7, mas também o intervalo que compreende $6.7 - 2.4 = 4.3$ ($DP = 2.4$) (Figura 3(a)).

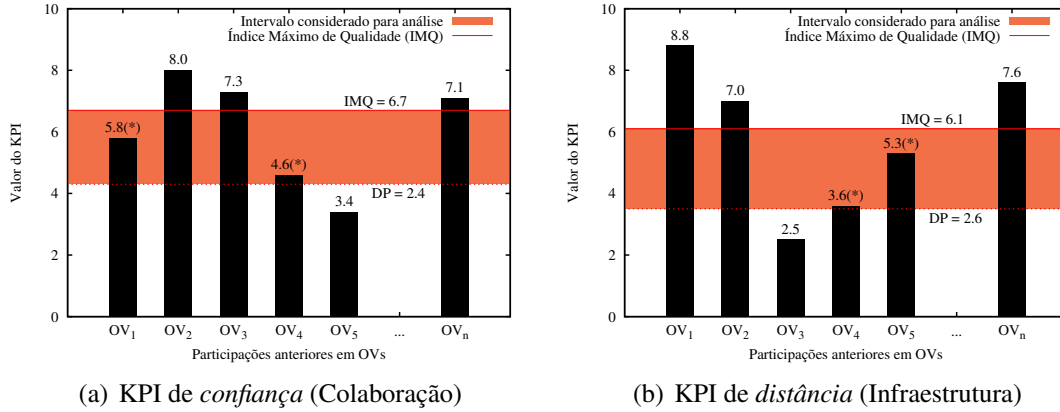


Figura 3. Valores históricos para os KPIs de confiança e distância de um PS.

Os valores atribuídos para cada KPI de cada grupo estão normalizados e podem variar de 0 a 10, associados à probabilidade de sucesso que varia entre 0 e 1, respectivamente. Assim, assumindo que cada PS participou de N_{PA} OVs anteriores e que n_R representa o número de participações anteriores de um PS em OVs em que os seus valores de KPIs são superiores a $IMQ_k^G - DP_k^G$ (marcados com um asterisco nas Figuras 3(a) e 3(b)), a Equação 3 calcula a probabilidade de sucesso dos KPIs para a participação atual.

$$Pr(K) = \frac{n_R}{n_{PA}} \quad (3)$$

A probabilidade de falha para um determinado KPI é representado como $Pr(\bar{K})$ pela seguinte equação:

$$Pr(\bar{K}) = 1 - Pr(K) \quad (4)$$

De acordo com a Figura 2, as probabilidades de sucesso e falha são calculadas para todos os dois grupos de KPIs que compõem as ETs de Colaboração (ET superior) e de Infraestrutura (ET inferior) de um PS, que são representadas por dois grupos de três eventos (KPIs) intermediários (e independentes uns dos outros) que preenchem as duas ETs. O evento K_2^1 , por exemplo, está relacionado ao KPI de comunicação (ET de Colaboração), com as probabilidades de sucesso e insucesso em $P(K_2^1)$ e $1 - P(K_2^1)$, respectivamente. Já o evento K_3^2 está relacionado ao KPI de *jitter* (ET de Infraestrutura), com as probabilidades de sucesso e insucesso em $P(K_3^2)$ e $1 - P(K_3^2)$, respectivamente.

Depois de atribuir todas as probabilidades para todos os ramos de cada uma das duas ETs, é necessário identificar se os PSs são minimamente qualificados para compor uma OV. Para isso, é realizado um cálculo para obter as probabilidades finais para todas

as combinações de eventos que compõem as ETs. No método ETA, os eventos ocorrem de forma independente, ou seja, onde a ocorrência de um evento não afeta a ocorrência de outro evento. Assim, elas são determinadas para cada um dos $2^{|K|}$ ramos de cada ET através da multiplicação das probabilidades de eventos que compõem cada caminho. A partir do conjunto de resultados obtido em cada uma das ETs, aplica-se o produto escalar nos resultados obtidos nos dois conjuntos para obter o nível de risco de cada PS.

Os conceitos apresentados podem ser formalizados da seguinte forma:

Seja $PS = \{PS_1, PS_2, \dots, PS_n\}$ um conjunto de n PSs previamente selecionados, onde cada elemento deste conjunto está associado a um tipo diferente de atividade de serviço que está sendo solicitado. Seja $K^G = \{K_1^G, K_2^G, \dots, K_m^G\}$ um conjunto de m KPIs, onde para $G = 1$ tem-se associado os m KPIs de Colaboração e para $G = 2$ tem-se associado os m KPIs de Infraestrutura, todos eles associados a um PS_n , e $\rho(K^G)$ a função de probabilidade associada a cada evento em K^G (como definido na Equação 3).

Agora, considere $P^G = \{P_1^G, P_2^G, \dots, P_{2^{|K|}}^G\}$ como um conjunto de todos os resultados possíveis das $2^{|K|}$ combinações entre $|K|$ (número de elementos em K) eventos de cada ET. O procedimento para a obtenção deste conjunto foi realizado utilizando uma Árvore de Busca Binária (ABB) [Bentley 1975], que percorre $2^{|K|}$ caminhos diferentes e atribui um valor para cada elemento de P^G , como mostrado na Equação 5:

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

onde P_{EI} é a probabilidade inicial do PS_n . A função ω , apresentada na Equação 6, corresponde a um vetor de 4 dimensões que realiza uma busca binária em cada árvore, retornando um elemento do caminho a cada iteração. Os valores i e j correspondem aos índices de início e fim da busca e possuem valores iniciais de $i = 0$ e $j = 2^{|K|}$, respectivamente. O valor k corresponde ao índice do elemento buscado (um elemento de P^G) e o elemento l ao nível atual da árvore. A sequência dos eventos pode ser visualizada nas duas ETs no Estágio 1 da Figura 2.

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

onde $c = (i + j)/2$. Após serem definidas para um PS_n todas as possíveis saídas P^G e calculadas suas respectivas probabilidades, aplica-se um cálculo de produto escalar sobre todos os elementos P^1, P^2, \dots, P^G (nesse artigo, apenas P^1 e P^2), como formalizado na Equação 7. A utilização do produto escalar como operação entre os diferentes conjuntos P é justificada pela possibilidade da ocorrência simultânea entre dois eventos iguais, porém em ETs diferentes. Por exemplo, supondo que no Estágio 1 da Figura 2, $P_1^1 = 0.7$ (ET de Colaboração), o que representaria uma probabilidade de 70% de chance de a combinação de três eventos (sucesso para K_1^1, K_2^1 e K_3^1) ocorrerem. De maneira semelhante, se $P_1^2 = 0.8$ (ET de Infraestrutura), significaria que a mesma sequência de eventos (sucesso para K_1^2, K_2^2 e K_3^2) também ocorreu. Assim, empregando-se o produto escalar entre os (dois) conjuntos P^1 e P^2 , pode-se obter o nível de risco final do provedor de serviço PS_n (que é representado por S_n):

$$S_n = P^1 \cdot P^2 \cdot \dots \cdot P^G = \sum_{i=1}^{2^{|K|}} P_i^1 P_i^2 \dots P_i^G \quad (7)$$

Os valores finais das probabilidades obtidas pela Equação 7 irão ser usados para medir e analisar o risco do PS coletivamente.

3.2. Análise de Risco Coletiva

O segundo estágio do método MAR-SP agrega os resultados providos pelo primeiro estágio (isto é, o nível de risco S_n de cada PS pré-analisado) para calcular o nível global de risco da OV, aplicando para isso o método AHP (*Analytic Hierarchy Process*) [Saaty 1996] como pode ser visualizado no Estágio 2 da Figura 2. No método AHP, os problemas estão dispostos em uma hierarquia, que tem início a partir do elemento mais geral (geralmente o objetivo) para os mais específicos (geralmente as alternativas). Neste trabalho, o AHP é modelado de maneira simplificada através de dois componentes: o objetivo e as alternativas. O objetivo do método AHP consiste em determinar o nível global de risco da OV. As alternativas consistem nos níveis de risco individuais de cada PS (S_n), obtido através da análise de risco individual (Estágio 1 da Figura 2).

Para cada alternativa S_i há também um peso W_i correspondente, que determina o grau de importância de cada PS_i sendo analisado em relação à OV. Por exemplo, dado uma OV sendo formada a partir de três PSs (como ilustrado na Figura 2), cada PS terá um nível de importância (peso) dentro da OV. Nesse sentido, o usuário pode alterar os pesos W_i de acordo com o grau de importância que será atribuído a cada PS_i que irá compor a OV. Estas características aumentam a robustez do método em relação às demais técnicas, determinando coletivamente a influência que cada PS possui dentro da OV e como o nível de risco de cada um deles irá impactar no nível de risco geral da OV. Nesse sentido, W_1, W_2, \dots, W_n é o peso de cada alternativa S_1, S_2, \dots, S_n associada ao objetivo. O objetivo geral (medir o nível de risco da OV) é representado por R_{OV} cujo procedimento de cálculo simplificado é apresentado na Equação 8:

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

A partir do cálculo apresentado na Equação 8, obtêm-se o nível global de risco na formação da OV particular ou em questão, considerando a importância de cada PS no processo.

4. Avaliação

Esta seção apresenta os resultados parciais obtidos até o momento desta pesquisa exploratória, que busca realizar um estudo de simulação, tomando como base os resultados preliminares obtidos em [Fiorese et al. 2012], a fim de adicionar o contexto de análise de risco. As próximas subseções apresentam os principais resultados obtidos.

4.1. Protótipo Computacional

Para viabilizar a implementação e geração dos resultados, foi desenvolvido um protótipo computacional, que integra as funcionalidades providas pelo modelo BPSS e pelo método

de análise de risco proposto nesse trabalho (MAR-SP). O protótipo desenvolvido foi dividido em dois módulos: módulo BPSS (*Best Peer Selection Service*) [Fiorese et al. 2012] e módulo DFRA (*Decision Framework for Risk Analysis*). O primeiro módulo implementa o modelo BPSS desenvolvido por [Fiorese et al. 2010, Fiorese et al. 2012] (ver Seção 2.1), utilizando o simulador de eventos discretos PeerFactSim.KOM [Stingl et al. 2011] como suporte para a criação da infraestrutura P2P SON e para possibilitar o processo de busca e seleção dos PSs. Já o módulo DFRA tem como foco específico a simulação de métodos de análise de risco, onde agrupa os PSs pré-selecionados pelo módulo BPSS em potenciais OVs a serem avaliadas pelo método MAR-SP.

No que diz respeito às especificações técnicas do sistema, o protótipo foi construído e os testes foram desenvolvidos em um computador Intel Core i5 3.1GHz, 4.0GB de memória RAM e Linux Mint 14.1 distribuição de 64 bits.

4.2. Estratégias de Simulação

As estratégias de simulação adotadas para o cenário de análise de risco seguem as mesmas estratégias utilizadas para a seleção dos PSs, ou seja, os dados foram obtidos a partir do projeto CAIDA e do banco de dados MaxMind GeoIP [Caida 2013]. Os PSs são representados por um conjunto de pares SON pré-selecionados cujos identificadores (endereços IPs) pertencem a cinco domínios geográficos, correspondentes a cinco países (Portugal, Espanha, França, Itália e Alemanha). Eles também são distribuídos igualmente entre as cinco áreas já mencionadas.

Os valores dos KPIs de Colaboração atribuídos para cada PS seguem uma distribuição linear que varia de 0 a 1, com intervalos de 0.01, sendo gerados durante o procedimento de simulação. Os valores dos KPIs de Infraestrutura são baseados em dados reais de cada PS obtidos a partir do banco de dados MaxMind GeoIP. Considera-se também que cada PS participou de 10 OVs anteriores (em média) quando ele foi selecionado. Por uma questão de simplicidade, a importância de cada PS em relação à OV será distribuída de maneira igualitária, considerando que a OV em questão será formada por apenas 3 PSs, ou seja, todos os PSs possuirão a mesma importância na OV ($W_1 = W_2 = W_3 = 0.33$). O intervalo de valores que determina o nível de risco de sucesso de uma OV (representada por um dentre 100 possíveis valores) será generalizado pelas seguintes notas de avaliação [Li and Liao 2007]: [0.0; 0.25]: muito baixo (L_1); [0.25; 0.50]: relativamente baixo (L_2); [0.50; 0.75]: relativamente alto (L_3); [0.75; 1.00]: muito alto (L_4). Por exemplo, uma OV com um nível global de risco $R_{OV} = 0.23$ será expressada pela nota L_1 (muito baixo).

4.3. Resultados

Os resultados apresentados nesta seção tem como objetivo avaliar, através da aplicação do método MAR-SP, o nível de risco para cada OV (conjunto de PSs) previamente formada no processo de seleção. Os procedimentos para a avaliação dessas OVs são divididos em duas fases: 1) Executar o processo de busca e seleção dos PSs através do módulo BPSS. Neste trabalho, o processo para a formação de uma OV levará em conta um conjunto de três PSs distintos que irão fornecer os seguintes serviços: VPN (PS_1), *Billing* (PS_2) e *Video-streaming* (PS_3); 2) Utilizar como entrada os três PSs selecionados na primeira fase e agrupá-los em um consórcio para medir (através dos KPIs de Colaboração e de Infraestrutura) qual nível de risco terá a possível OV a ser formada por eles.

A Tabela 1 apresenta os resultados de uma simulação que contempla a avaliação de 100 OV's formadas a partir de um cenário com 300 PS's em uma P2P SON. Para viabilizar essa simulação, foram executadas 100 vezes a primeira e segunda fase anteriormente mencionadas, resultando em 100 possíveis OV's a serem analisadas. Além disso, cada simulação foi repetida 10 vezes a fim de se obter valores médios (incluindo o desvio padrão) para o nível de risco de cada OV. Os resultados obtidos mediante o nível de risco apresentado por cada OV (em percentual) foram agrupados em quatro escalas de avaliação (L_1 , L_2 , L_3 e L_4), como apresentado na Tabela 1.

	Escalas de Risco para as OV's			
	Muito baixo (L_1)	Rel. baixo (L_2)	Rel. alto (L_3)	Muito alto (L_4)
Risco (em %)	21.37	40.43	27.04	11.16
Desvio Padrão	2.98	3.54	1.89	1.06

Tabela 1. Distribuição do nível de risco para 10 simulações envolvendo 100 OV's.

A partir dos resultados apresentados na Figura 1, verifica-se que a maior parte das OV's que foram avaliadas possuem um nível de risco muito baixo (21.37%) ou relativamente baixo (40.43%). Isso ocorre pois, por exemplo, um PS pode apresentar bons indicadores de infraestrutura, no entanto não possuir a colaboração necessária para assegurar um bom desempenho da OV e vice-versa. Neste sentido, pode-se concluir que o método favorece uma avaliação mais rigorosa quando há um aumento no número de indicadores, e que portanto, deve ser levado em conta uma maior prevenção e controle do risco, a fim de proporcionar maior segurança em uma futura operação da OV.

5. Conclusão

Este artigo consiste em uma pesquisa exploratória que abordou temas relacionados com a identificação e a mensuração do risco em OV's. De modo geral, a análise de risco tornou-se um elemento chave no planejamento de uma OV, dado que pequenos erros podem comprometer sua eficiência como um todo. Por esta razão, foi proposto um novo método para realizar a análise de risco sobre um conjunto de Provedores de Serviços (PS's) que vão compor uma Organização Virtual (OV). O presente método, chamado MAR-SP, é composto por duas fases. A primeira delas realiza a análise de risco individual para cada PS pré-selecionado, através do método ETA (*Event Tree Analysis*). Tendo como entrada os resultados da primeira fase, a segunda fase calcula e analisa o risco global, considerando os PS's coletivamente, utilizando para isso o método AHP (*Analytic Hierarchy Process*).

A fim de avaliar o comportamento do método MAR-SP, seis KPI's distintos, sendo três deles relativos aos aspectos de colaboração entre os PS's (confiança, comunicação e comprometimento) e três deles relativos aos aspectos de infraestrutura de redes P2P (distância, atraso e *jitter*) foram considerados na análise para cada PS. As simulações realizadas envolveram diversos conjuntos de PS's pré-selecionados, que foram analisados a partir dos resultados de [Fiorese et al. 2012]. Os resultados obtidos se mostraram promissores sobre a conveniência do método quanto à sua finalidade. O grau de desempenho necessário para cada PS compor uma OV é alto e é fortemente influenciado tanto pelos aspectos de colaboração entre os PS's quanto pela própria infraestrutura da rede na qual os PS's estão conectados. Assim, para que uma OV seja efetivamente formada, deve-se levar

em conta PSs que, além de possuírem maior qualidade no quesito colaboração, também apresentem qualidade exigida de serviço de rede.

Da mesma maneira, o método apresentado contribui para uma forma mais concreta e sistematizada de expressar, medir, avaliar e mitigar os riscos na formação de uma OV, tanto a nível individual como coletivamente, apesar de nesse trabalho se concentrar apenas em PSs. Além disso, a utilização do método no processo de análise de risco permite realizar uma avaliação com maior transparência e com um nível muito menor de subjetividade, descartando ou não os PSs, antes de compor uma OV, de acordo com os critérios estabelecidos. Os próximos passos a partir dos resultados obtidos nesse trabalho incluem a criação de um *framework* que engloba a análise de risco não apenas no processo de busca e seleção, mas que considera todos os aspectos para a formação de uma OV.

Referências

- Alawamleh, M. and Popplewell, K. (2010). Risk sources identification in virtual organisation. In *Enterprise Interoperability IV*, pages 265–277. Springer London.
- Alawamleh, M. and Popplewell, K. (2012). Analysing virtual organisation risk sources: an analytical network process approach. *International Journal of Networking and Virtual Organisations*, 10(1):18–39.
- Bentley, J. L. (1975). Multidimensional binary search trees used for associative searching. *Communications of the ACM*, 18(9):509–517.
- Caida (2013). Macroscopic topology project. <http://www.caida.org/analysis/topology/macroscopic/>.
- Camarinha-Matos, L. M. and Afsarmanesh, H. (2005). Collaborative networks: a new scientific discipline. *Journal of Intelligent Manufacturing*, 16(4-5):439–452.
- Camarinha-Matos, L. M. and Afsarmanesh, H. (2008). On reference models for collaborative networked organizations. *International Journal of Production Research*, 46(9):2453–2469.
- Duan, Z., Zhang, Z. L., and Hou, Y. T. (2003). Service overlay networks: SLAs, QoS, and bandwidth provisioning. *IEEE/ACM Transactions on Networking*, 11(6):870–883.
- Ericson, C. A. (2005). *Hazard analysis techniques for system safety*. John Wiley & Sons, New York, USA.
- Fiorese, A., Matos, F., Junior, O. C. A., and Ruppenthal, R. M. (2013). Multi-criteria approach to select service providers in collaborative/competitive multi-provider environments. *International Journal of Computer Science and Network Security*, 13(9):15–22.
- Fiorese, A., Simões, P., and Boavida, F. (2010). OMAN – a management architecture for P2P service overlay networks. In *Proceedings of the 4th international conference on Autonomous infrastructure, management and security (AIMS'10)*, pages 14–25, Zurich, Switzerland.
- Fiorese, A., Simões, P., and Boavida, F. (2012). Peer selection in P2P service overlays using geographical location criteria. In *Proceedings of the 12th international conference on Computational Science and Its Applications (ICCSA'12)*, pages 234–248, Salvador de Bahia, Brazil.

- Goranson, H. T. (1999). *The agile virtual enterprise cases, metrics, tools*. Quorum Books, Westport, CT, USA.
- Grabowski, M. and Roberts, K. H. (1998). Risk mitigation in virtual organizations. *Journal of Computer-Mediated Communication*, 3(4):704–721.
- Junior, O. C. A. and Rabelo, R. J. (2013). A KPI model for logistics partners' search and suggestion to create virtual organisations. *International Journal of Networking and Virtual Organisations*, 12(2):149–177.
- Kaune, S., Pussep, K., Leng, C., Kovacevic, A., Tyson, G., and Steinmetz, R. (2009). Modelling the internet delay space based on geographical locations. In *Proceedings of the 17th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP'09)*, pages 301–310, Weimar, Germany.
- Li, Y. and Liao, X. (2007). Decision support for risk analysis on dynamic alliance. *Decision Support Systems*, 42(4):2043–2059.
- March, J. G. and Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, 33(11):1404–1418.
- Montgomery, D. C. and Runger, G. C. (2011). *Applied Statistics and Probability for Engineers*. John Wiley & Sons, New Jersey, USA.
- Mowshowitz, A. (1997). Virtual organization. *Communications of the ACM*, 40(9):30–37.
- Neely, A., Richards, H., Mills, J., Platts, K., and Bourne, M. (1997). Designing performance measures: a structured approach. *International Journal of Operations & Production Management*, 17(11):1131–1152.
- Pidduck, A. B. (2006). Issues in supplier partner selection. *Journal of Enterprise Information Management*, 19(3):262–276.
- Saaty, T. L. (1996). *Decision making with dependence and feedback: The analytic network process*. RWS Publications, Pittsburgh, USA.
- Saaty, T. L. (2004). Decision making – the analytic hierarchy and network processes (ahp/anp). *Journal of Systems Science and Systems Engineering*, 13(1):1–35.
- Stingl, D., Gross, C., Ruckert, J., Nobach, L., Kovacevic, A., and Steinmetz, R. (2011). PeerfactSim.KOM: a simulation framework for peer-to-peer systems. In *Proceedings of the 13th International Conference on High Performance Computing and Simulation (HPCS'11)*, pages 577–584, Istanbul, Turkey.
- Vose, D. (2008). *Risk analysis: a quantitative guide*. John Wiley & Sons, New Jersey, USA.
- Zhou, S., Hogan, M., Ardon, S., Portman, M., Hu, T., Wongrujira, K., and Seneviratne, A. (2005). Alasa: When service overlay networks meet peer-to-peer networks. In *Proceedings of the 11th Asia-Pacific Conference on Communications (APCC'05)*, pages 1053–1057, Perth, Australia.