Uso de um Modelo de Confiança para a Composição de Serviços Web*

Emerson Ribeiro de Mello[1,2], Joni da Silva Fraga[1], Michelle Silva Wangham[3]

[1]Departamento de Automação e Sistemas
Universidade Federal de Santa Catarina (UFSC) – Florianópolis, SC

[2]Instituto Federal de Santa Catarina (IFSC) – São José, SC

[3]Grupo de Sistemas Embarcados e Distribuídos – GSED/CTTMAR
Universidade do Vale do Itajaí (UNIVALI) – São José, SC

{emerson,fraga}@das.ufsc.br, wangham@univali.br

Abstract. *Business process-oriented services are crossing organizational boundaries and are provided by different partners. This work defines a probabilistic trust model that aims dynamic trust establishment between business partners, even in front of entities that do not have any previous link. The proposed model is based on a distributed reputation system that offers ways to assist the process of selecting partners through a Bayesian analysis.*

Resumo. *Processos de negócios orientados a serviços são constituídos por serviços que transpassam os limites organizacionais e são providos por diferentes parceiros. Este artigo define um modelo de confiança probabilista que permite o estabelecimento dinâmico da confiança entre parceiros de negócios, mesmo diante de entidades que não possuam qualquer vínculo anterior. O modelo proposto está fundamentado sobre um sistema de reputação distribuído que fornece suporte ao processo de seleção de parceiros através de uma análise bayesiana.*

1. Introdução

Nas redes colaborativas, a criação de processos de negócios sob demanda requer uma composição de Serviços *Web* que seja dinâmica, auto-gerenciada e segura. A composição dinâmica de Serviços *Web* normalmente está baseada sobre um conjunto de dados semânticos os quais descrevem as funcionalidades de cada serviço. Tais dados são então usados na criação dinâmica de processos de negócios, podendo ainda ser usados na geração de sequências de orquestração [Wu et al. 2003].

Órgãos padronizadores propuseram diversas especificações para tratar as questões básicas de segurança como a integridade, confidencialidade e a autenticidade [Bartel et al. 2002, Imamura et al. 2002, OASIS 2004b, WS-Trust 2005]. Entretanto, quando se considera não mais um serviço único, mas sim uma composição dinâmica de Serviços *Web*, constata-se que a segurança dos processos de negócios não fora ainda

*Trabalho desenvolvido dentro do escopo do projeto "Mecanismos de Segurança para Processos de Negócios em Redes Colaborativas" (CNPq 484740/2007-5)

profundamente investigada e que ainda não existem soluções concretas e completas [Charfi and Mezini 2005, Carminati et al. 2005].

Em segurança computacional, o termo confiança geralmente restringe-se a garantir a identidade das partes que estão se relacionando. No atual cenário da Arquitetura Orientada a Serviços (AOS), é comum que se tenha diversos provedores de serviços oferecendo muitas vezes serviços similares e tratar a confiança nessas redes colaborativas tão e somente como garantir a identidade de uma entidade, seja esta um cliente ou um provedor de serviços, pode não ser suficiente. Nestes ambientes complexos, com interações momentâneas e fracamente acopladas, surge então a necessidade de um gerenciamento de confiança para auxiliar, por exemplo, um cliente a decidir, entre os similares, com qual provedor interagir.

Segundo [Khare and Rifkin 1998], inconsistências nas atuais relações de confiança em sistemas de larga escala, indicam a necessidade de funções para um gerenciamento flexível destas relações, o que permitiria a navegação por complexas redes de confiança que se caracterizam por relações dinâmicas. Em [Grandison and Sloman 2000], o gerenciamento de confiança é caracterizado pela coleta de informações necessárias para estabelecer novas relações de confiança além de monitorar e reavaliar tais relações durante a evolução das interações de uma aplicação distribuída.

O ponto crítico das redes de confiança está no estabelecimento inicial da confiança entre duas entidades (parceiros do processo de negócio) que não se conhecem. Ambas entidades se arriscam em uma relação inicial sem qualquer respaldo. As soluções apresentadas na literatura para tal problema consistem geralmente no uso de sistemas de reputações, através de provedores de opiniões, que torna possível avaliar a probabilidade das partes honrarem as atividades.

Esta probabilidade, ou a medida da confiança, é basicamente calculada de duas formas: através de médias ponderadas [Gray et al. 2003, Wang and Vassileva 2003, Sabater and Sierra 2001] ou através de métodos estatísticos [Buchegger and Le Boudec 2004, Whitby et al. 2005, Teacy et al. 2006]. Os trabalhos que usam média ponderada normalmente atribuem um peso para cada provedor de opiniões (base de reputação), ou seja, as informações recebidas de provedores de opiniões considerados mais confiáveis terão uma maior influência no valor final sobre a confiança calculada para um dada entidade do que aquelas oriundas de provedores considerados menos confiáveis. Os métodos estatísticos fazem uso das interações passadas para prever como será o comportamento futuro, tanto dos provedores de opiniões quanto da entidade para qual se deseja formar um novo valor de confiança.

Para que o processo de seleção de parceiros, em uma composição de serviços, não se limite a explorar os registros UDDI [OASIS 2004a], o uso de descritores semânticos de Serviços *Web* como, por exemplo, a linguagem OWL-S (OWL-based Web Service Ontology) [Martin et al. 2004], são ideais para fornecer competências para anotações de dados semânticos dos serviços. Para [Carminati et al. 2005], a segurança assume um papel importante na seleção dinâmica de parceiros, sendo a confiança o principal fator de influência em tal processo. Assim, de nada adianta realizar inferências sobre as ontologias dos serviços para selecionar os participantes que irão compor o processo, se não há confiança nos respectivos provedores.

É neste cenário que o presente trabalho propõe uma solução. É apresentada uma forma de agrupamento de entidades (usuários, provedores de serviços) e o uso de um modelo de confiança probabilista para a tomada de decisões sobre interações entre parceiros da rede colaborativa. Na literatura, modelos de confiança estão sempre combinados com modelos de reputação e o presente trabalho segue esta linha. A decisão de um parceiro confiar ou não em um outro parceiro é tomada com base nas experiências passadas entre estes. Caso não haja tais experiências, são requisitadas opiniões de outros parceiros da rede colaborativa para assim formar um valor de confiança e a partir deste, determinar se é possível realizar a negociação.

2. Modelo de Confiança Federado

Os Serviços *Web* compostos estão inseridos em ambientes caracterizados pela grande quantidade de entidades participantes, sejam estas clientes ou provedores de serviços. As soluções de segurança em tais ambientes, como o provimento de controles de autenticação e de autorização, devem ser escaláveis.

O uso de modelos de segurança federados é fundamental para resolver os problemas intrínsecos aos ambientes de larga escala, pois em tais modelos são definidas infra-estruturas para sistemas de identificação e de autenticação próprios. Mas, nos sistemas atuais uma federação pode cobrir somente uma pequena parte (um pequeno grupo de entidades) de uma aplicação distribuída. O relacionamento entre federações garante ao modelo o conceito de visibilidade global, permitindo que entidades de uma federação (parceiros de um processo de negócio) possam interagir com entidades (parceiros) de outras federações em uma composição de serviços.

O modelo de segurança apresentado neste trabalho agrupa clientes e provedores de serviços em federações. Cada federação é regida por uma entidade denominada **gerente** que tem por objetivo gerenciar seus membros além de estabelecer e manter relações de confiança com gerentes de outras federações. O gerente atua como uma Terceira Parte Confiável (TPC), a qual é responsável por emitir e validar credenciais de segurança, podendo este ser invocado por entidades membros de sua federação ou não. As relações entre federações permitem que credenciais emitidas por um gerente em uma federação sejam consideradas válidas por um provedor de serviços de uma outra federação.

Nesta proposta, cada federação representa um domínio onde os membros são regidos por uma política de negócios comum. A confiança existente do gerente sobre seus membros é binária, ou seja, se um cliente ou provedor de serviços é membro da federação, então isso indica que este cumpre todos os requisitos definidos pelo gerente e sendo assim é considerado confiável. Por outro lado, as relações de confiança entre gerentes seguem uma abordagem difusa, permitindo expressar diferentes níveis de confiança.

O fato dos membros fazerem parte de uma mesma federação não implica que estes membros possuam confiança entre si. Porém, implica que estes membros estão associados por algum tipo de afinidade e isto pode ser um fator de influência para favorecer o estabelecimento das relações de confiança entre os mesmos na federação. Neste trabalho, as relações de confiança não são simétricas e não são transitivas, ou seja, “a” confia em “b” não implica que “b” confie em “a”. E “b” confia em “c” não implica que “a” confie em “c”. Por fim, as relações de confiança entre as entidades são arbitrárias e não se restringem aos limites da federação, como visto na Figura 1. Neste exemplo, a entidade “a”

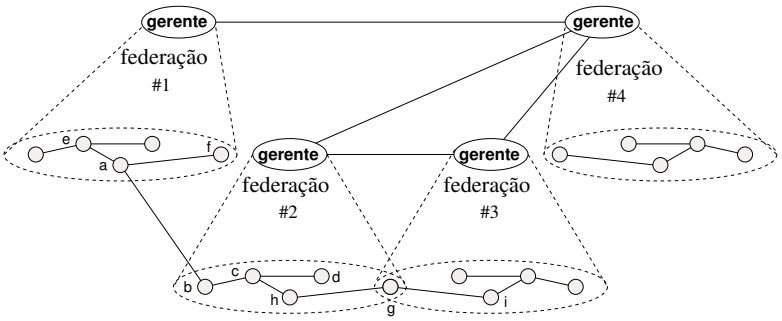


Figura 1. Relações de confiança: inter e intra-federação

possui relações de confiança com "e" e "f", ambas pertencentes à mesma federação de "a", e com a entidade "b", esta pertencente a uma outra federação.

Para o estabelecimento de novas relações de confiança, sejam estas entre membros ou entre gerentes de federações, é proposto neste trabalho um sistema de reputações que é alimentado pelas relações de confiança já existentes. O sistema de reputação é constituído de forma distribuída, isto é, não existe uma base de reputação centralizada a qual todas as entidades do sistema alimentam e utilizam. Cada entidade membro possui uma *base de conhecimento* individual que agrega informações oriundas de experiências diretas e opiniões providas por outras entidades, sejam estas recebidas de outros membros ou dos gerentes das federações das quais pertença. Tal abordagem permite que cada entidade do sistema tenha uma visão particular da rede de confiança.

Apesar da *base de conhecimento* ser individual a cada entidade, a mesma se faz disponível através dos gerentes das federações. Isso retira dos membros a complexidade em gerenciá-las, porém não impede a visão particular que cada entidade possui do sistema de reputações. Na Figura 1, clientes e provedores de serviços podem pertencer a mais de uma federação e para estes casos, a *base de conhecimento* de tais entidades fica replicada por cada um dos gerentes das federações que estas entidades pertençam. Tal replicação possui dois papéis importantes no modelo: (1) evita um ponto único de falhas; (2) permite que as experiências de dada entidade esteja disponível para um número maior de entidades.

No modelo proposto, os gerentes não possuem papel ativo, ou seja, estes não interagem com outros membros de forma que mantenham uma base própria de experiências diretas. Diferentemente dos membros que fornecem opiniões com base em suas experiências anteriores, os gerentes necessitam fazer uso das bases de experiências de seus membros para também fornecer opiniões.

As opiniões providas pelo gerente são interessantes para casos no qual uma entidade a deseja conhecer a reputação de uma entidade d e não encontra na sua *base de conhecimento* (experiências diretas e opiniões de outros membros) qualquer informação a respeito da entidade desejada (d). Assim, a entidade a requisita ao seu gerente opiniões sobre d para que este combine todas as experiências que seus membros tiveram para então encaminhar para a um valor já formado. A Figura 2 ilustra as bases de experiências dos membros (A, B, C e D) dispostas no gerente da federação. Cada membro registra em sua base se as interações que teve com outras entidades resultaram em sucesso ou insucesso (sistema detalhado na Seção 2.1).

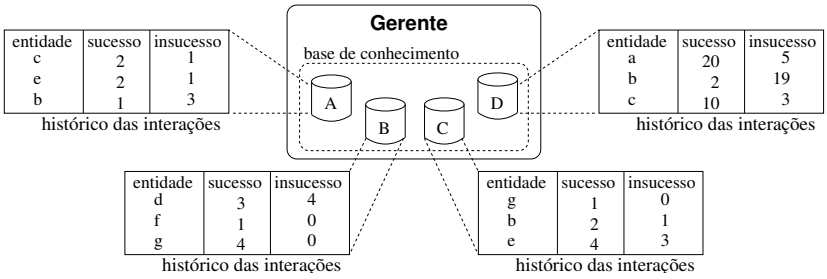


Figura 2. Bases de experiências dos membros dispostas no gerente

O uso de opiniões de membros oriundas de uma única federação não garante a visibilidade global. Por exemplo, um membro da federação 1 (ver Figura 1) deseja consultar a reputação da entidade d, que faz parte da federação 2. Ao consultar o gerente da federação 1, o requisitante de informações constata que nenhum outro membro de sua federação possui opinião sobre d. Para este caso, as relações de confiança entre federações permitem que um gerente propague a consulta pelos demais gerentes, através destas relações, garantindo assim a visibilidade global das informações sobre reputações.

2.1. Sistema de Confiança e Reputação

Em um processo de negócio, a interação de um provedor i com um serviço do provedor j está condicionada a probabilidade deste último honrar a negociação. Tal probabilidade é calculada com base nas experiências diretas entre *i* e *j*, realizadas anteriormente, e, no caso da ausência destas experiências, *i* poderá requisitar opiniões de outras entidades acerca de *j*, inclusive aos seus gerentes.

Como nos demais trabalhos da literatura [Buchegger and Le Boudec 2004, Whitby et al. 2005, Teacy et al. 2006], optamos por uma análise bayesiana para determinar a probabilidade de uma entidade *j* honrar futuras interações. Nos sistemas bayesianos, para determinar a probabilidade (*a posteriori*) de *j* honrar as futuras interações é necessário conhecer a probabilidade *a priori*, sendo que esta pode ser obtida através de uma *função densidade de probabilidade* de uma *distribuição beta*[1] (Equação 1).

$$f(p) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}, \text{ sendo } \alpha, \beta > 0 \quad (1)$$

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt \quad (2)$$

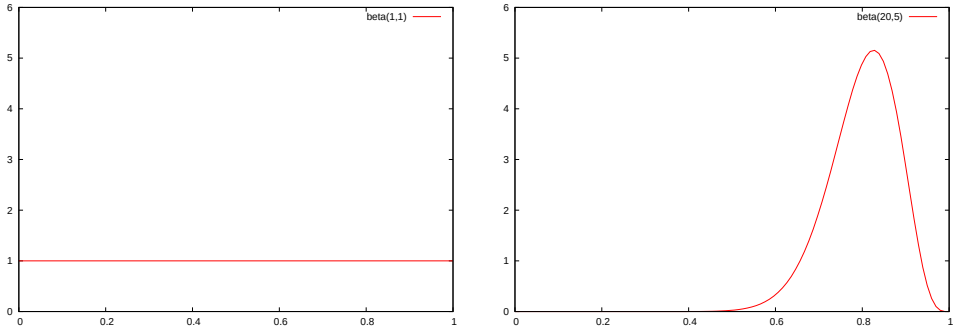
sendo $\Gamma(x)$ a função Gama de Euler que estende a noção de fatorial para valores não inteiros.

O fato de só precisar de dois parâmetros (α e β), que são atualizados de forma contínua, torna a *distribuição beta* atrativa em sistemas Bayesianos para calcular a probabilidade de uma entidade honrar uma negociação. Segundo [Buchegger and Le Boudec 2004], os parâmetros α e β são usados como probabilidade *a priori* e, no modelo proposto, estes parâmetros funcionam como registros do total de

[1]Uma *distribuição beta*, determinada pelos parâmetros α e β, é usada para representar variáveis aleatórias que são limitadas dentro de um intervalo, por exemplo, entre 0 e 1 [Jain 1991].

interações entre os provedores i e j que resultaram em sucesso e insucesso, respectivamente.

Sistemas de reputações tornam-se mais precisos quando suas bases possuem grandes quantidades de registros. Porém, em seu início uma base de informação é nula. Considerando o exemplo anterior, no qual o provedor i deseja calcular a probabilidade do provedor j honrar a próxima interação e sabendo que não existe qualquer experiência anterior entre i e j, tem-se os seguintes valores para os parâmetros de registro de i: $\alpha = totalSucesso + 1$ e $\beta = totalInsucesso + 1$. Assim, no início é assumido uma distribuição uniforme sendo que a probabilidade de qualquer interação ocorrer com sucesso ou sem sucesso é exatamente igual, isto é, a probabilidade de j honrar ou não uma requisição de serviço de i será exatamente igual (ver Figura 3(a)).



(a) distribuição beta(1,1) (b) distribuição beta(20,5)

Figura 3. Distribuição beta

A partir do momento que novas observações são realizadas por i sobre as interações com j, os valores de α e β são atualizados, o que resultará em uma probabilidade *posteriori* mais expressiva. A Figura 3(b) ilustra um caso em que 19 interações resultaram em sucesso e 4 resultaram em insucesso ($\alpha = 19 + 1$ e $\beta = 4 + 1$). Por fim, a probabilidade p do provedor j honrar a interação é calculada através do *valor esperado* $E(p)$ da distribuição beta (Equação 3), que para o caso da Figura 3(b) é igual a $0,8$. Uma vez calculada a probabilidade de j honrar a interação, cabe ao provedor i determinar, de forma subjetiva, se o valor obtido é suficiente para que este possa interagir com j.

$$E(p) = \frac{\alpha}{\alpha + \beta} \tag{3}$$

Determinar o grau de confiança em um provedor consiste também em considerar o contexto no qual tal provedor está inserido. A delimitação do contexto serve para expressar a confiança com uma maior precisão, pois um provedor pode atuar em diferentes contextos e para cada um destes o mesmo pode assumir diferentes comportamentos. Por exemplo, um provedor oferece um serviço para previsões do tempo e um serviço para indicar as melhores empresas na bolsa de valores para se investir. Das diversas interações com o provedor foi observado que as previsões do tempo fornecidas sempre foram precisas, porém as indicações sobre empresas nem sempre resultaram em sucesso. O provedor de serviços, portanto, pode possuir uma boa reputação no contexto de “previsões do tempo”, entretanto, o mesmo pode não ser verificado no contexto de “investimentos financeiros”.

No modelo de confiança proposto, informações de contexto também são consideradas. Cada entidade possui uma base de experiências diretas, que contém os históricos das interações que realizou com as demais entidades. As experiências registradas são separadas por contexto e com isto é possível determinar em quais contextos o provedor se mostrou mais correto. Caso não exista qualquer experiência em um determinado contexto, a combinação de todas as experiências, não importando o contexto, pode ajudar no provimento de informações para o contexto desejado. As interações seguintes, dentro do contexto desejado, aprimoram esta visão inicial da confiança.

2.1.1. Estabelecimento da Confiança

Para i determinar a probabilidade do provedor de serviços j honrar uma futura interação, é necessário inicialmente analisar as experiências anteriores entre os mesmos. Mas, nem sempre é possível assumir a existência de experiências diretas e uma forma de atacar este problema é através de sistemas de reputações. Neste trabalho, i obtém opiniões de entidades com quem possui relações de confiança estabelecidas, sejam estas membros ou gerentes de federações. Estas bases constituem a *base de conhecimento* da entidade i.

Um provedor i que deseja formar um valor de confiança para o provedor de serviços j, consulta sua base de relações, procurando opiniões sobre j. Cada entidade k, que possui relações com i, fornecerá então o *valor esperado* (ver Equação 3) obtido sobre j. De posse destes valores, o provedor i deve agregá-los através da Equação 4.

$$c_{ij}^{s} = \frac{\sum_{k}^{y} co_{ik}^{s} \times op_{kj}^{s}}{\sum_{k}^{y} co_{ik}^{s}} \tag{4}$$

sendo c_{ij}^{s} o valor de confiança formado por i sobre o provedor de serviços j no contexto s. co_{ik}^{s} representa a confiança que i possui sobre o provedor de opiniões k no contexto s. op_{kj}^{s} expressa a opinião de k sobre j no contexto s. Assim, a Equação 4 mostra que as opiniões recebidas por i serão ponderadas de acordo com a confiança que i possui sobre os provedores de opiniões k. Por fim, cabe a i determinar, de forma subjetiva, se o valor c_{ij}^{s} é suficiente para que este possa interagir com o provedor de serviços j.

Como descrito na Seção 2.1, os gerentes também atuam como provedores de opiniões. O uso destes em tal tarefa é vantajoso pois reúnem uma quantidade maior de entidades provedoras de opiniões. As opiniões fornecidas pelos gerentes não são geradas a partir de experiências próprias, pois os gerentes não possuem papel ativo no modelo. Essas opiniões são obtidas através da combinação das experiências que seus membros tiveram com a entidade para quem se deseja conhecer a reputação. Um gerente pode ainda requisitar opiniões a outros gerentes, com quem possua um relacionamento, usufruindo da rede de confiança.

Dessa forma, a opinião de um gerente sobre um provedor j, consiste no valor esperado de uma distribuição beta com $\alpha = \sum_{l}^{m} a_{lj}^{s}$ e $\beta = \sum_{l}^{m} b_{lj}^{s}$, sendo a_{lj}^{s} o total de experiências com sucesso que o membro l teve com o provedor j dentro do contexto s; b_{lj}^{s} o total de insucessos; e m o número total de membros da federação em questão que

interagiram com j.

A opinião recebida de um gerente, ou de um conjunto de gerentes, é agregada de acordo com a Equação 4. Isto permite a entidade que está requisitando opiniões, determinar quais federações apresentaram opiniões mais precisas no decorrer do tempo, ou seja, cabe a esta entidade ponderar as opiniões recebidas de cada gerente.

3. Serviços Agregados ao Gerente

A interação entre membros e gerentes de uma federação é feita através de dois Serviços *Web* disponibilizados no gerente: o Serviço de Registro de Opiniões (SRO) e o Serviço Agregador de Opiniões (SAO). O primeiro é utilizado pelos membros das federações para que estes possam inserir registros em suas bases de experiências. Após o término de cada interação, um membro invoca seu SRO para registrar com qual entidade interagiu, em que contexto e, por fim, indica se a interação ocorreu com sucesso ou não.

O Serviço Agregador de Opiniões (SAO) é utilizado pelos membros para requisitar opiniões sobre uma dada entidade. Um membro pode invocar o SAO para: (1) verificar o resultado das experiências diretas que teve com uma dada entidade (sua base fica disposta no gerente); (2) obter opiniões de outras entidades com as quais já possua confiança; (3) obter uma opinião agregada de todos os membros de uma federação; e (4) para obter opiniões através de diversas federações.

O SRO permite que somente os membros adicionem novas informações às suas bases de conhecimento e operações como modificação e exclusão destas informações não são permitidas. Ou seja, um membro só pode incrementar o total de casos de sucessos e insucessos sobre uma outra entidade. Esse comportamento previne que um membro manipule sua própria base de conhecimento de forma que o SAO forneça diferentes opiniões para diferentes requerentes. Um exemplo deste tipo de ataque consiste de uma entidade maliciosa m que apesar de ter registrado que realizou n interações com sucesso com uma entidade e, consegue de alguma forma prever que uma entidade t, com quem também possui uma relação de confiança, pretende realizar negócios com e ou com f (seu parceiro). A entidade m poderia então modificar sua base de forma que t verifique que e não honrou as negociações com m, privilegiando assim f. Por fim, após tal consulta, m poderia modificar sua base de conhecimento de forma a não provocar suspeita e, se e consultá-la posteriormente, irá encontrar informações que de fato ocorreram, ou seja, m indicará que e honrou as n negociações.

O maior problema que um membro pode causar ao sistema de reputações é o registro de interações de forma maliciosa, por exemplo, registrando que uma interação ocorreu com insucesso, mesmo que na verdade esta tenha sido realizada com sucesso. A base de conhecimento desta entidade, apesar de ser incoerente, será a mesma para qualquer entidade que a consulte em qualquer momento e o sistema de reputação, apresentado na Seção 2.1, se encarregará de filtrar opiniões de entidades maliciosas. Ou seja, o uso de diversas fontes de opiniões aliado inclusive a fonte de experiências diretas entre a entidade consultora e a entidade para quem se está calculando a confiança, permitirá punir os maus provedores de opiniões. O provimento contínuo de opiniões incorretas fará com que um provedor malicioso não seja mais consultado.

4. Experimentos

Para verificar a efetividade do modelo de confiança proposto foram realizados experimentos em um ambiente simulado. A dinâmica das simulações consistiu primeiramente em escolher um provedor de forma aleatória, denominado "compositor de processos de negócios" e a partir deste escolher um conjunto de provedores, denominados "parceiros", que farão parte do processo de negócio (p. ex. uma orquestração de serviços).

Cada candidato a parceiro possui um comportamento próprio o qual indica como o mesmo irá se portar em cada interação que venha a participar. O comportamento de cada provedor foi escolhido de forma aleatória e este é representado por um número real dentro do intervalo de 0 a 1. Provedores com o $comportamento = 1$ honram todas as interações e com o $comportamento = 0$ não honram qualquer interação. Os valores intermediários são expressos a uma granularidade de $0,1$.

A seleção dos parceiros do processo está condicionada ao valor de confiança (ver Seção 2.1) calculado pelo compositor sobre os provedores candidatos a parceiros. A seleção só ocorrerá se o valor obtido for superior ao limiar definido pelo compositor. Nas simulações, foi adotado um limiar de $0,5$. Por fim, para cada cenário simulado foi contabilizado o total de interações que resultaram em sucesso e em insucesso. A Tabela 1 descreve os cenários analisados nas simulações.

Tabela 1. Cenários analisados nas simulações

Cenários	Descrição
1	O compositor de processos interage com os provedores candidatos a parceiros sem consultar qualquer base de reputações, não usando sequer sua própria base de reputação.
2	O compositor de processos armazena um histórico sobre o resultado das interações que teve com os provedores candidatos e esta base serve de ajuda na tomada de decisão para as futuras interações.
3	Antes de qualquer interação, o compositor de processos requisita opiniões de outros provedores com quem já possui alguma confiança. As opiniões recebidas determinam se o provedor será selecionado.
4	Antes de qualquer interação, o compositor de processos requisita opiniões aos seus gerentes.
5	O compositor de processos combina as informações contidas em sua própria base de reputações com as opiniões recebidas de provedores de opiniões e dos gerentes.

O vínculo entre membros e gerentes de federações e o agrupamento de federações constitui a rede de confiança em nosso modelo. E esta rede, por sua vez, pode ser vista como um grafo onde as entidades (membros ou gerentes) representam os vértices e as relações de confiança entre estas entidades formam os arcos. A topologia dessas redes de confiança apresenta uma forte influência na efetividade das buscas por opiniões, uma vez que os arcos entre os nós indicam como as opiniões devem ser propagadas.

De acordo com a literatura [Capkun et al. 2002], a topologia destas redes de confiança segue o conceito do mundo pequeno [Milgram 1967], com uma distribuição de acordo com a lei da potência [Albert and Barabási 2002]. Nas simulações realizadas, optou-se por usar o modelo proposto em [Albert and Barabási 2002] para gerar a topologia da rede e assim prover no ambiente simulado uma topologia próxima daquela que é encontrada na prática.

A simulação foi conduzida em uma rede com 300 entidades, sendo que 5% deste total são gerentes e as demais entidades são obrigatoriamente membros de duas federações quaisquer. Cada entidade membro (provedor) possui confiança estabelecida com 16 outras entidades, não necessariamente presentes na mesma federação que a entidade em questão. Para cada cenário apresentado acima, foram realizadas simulações com dois conjuntos de provedores candidatos, conforme apresentados na Tabela 2.

Tabela 2. Conjuntos de provedores utilizados nas simulações

Conjunto	Descrição
1	Provedores que nunca interagiram com qualquer provedor que tenha vínculo direto com o compositor de processos.
2	Provedores que já interagiram com algum provedor que possui vínculo direto com o compositor de processos.

Para cada cenário foram realizados 128 experimentos, independentes entre si, mas iguais em todos os cenários. Com o intuito de verificar o desempenho do modelo proposto em um ambiente próximo a um cenário real em produção, ou seja, um cenário onde as entidades já detivessem uma base de experiência formada, nas simulações realizadas todas as entidades da rede tiveram suas bases de reputações alimentadas através de interações entre si. O compositor de processos realizou interações com cada um dos provedores com quem possui vínculo direto e o total de interações com cada provedor foi determinado de forma aleatória dentro do intervalo de 1 a 128. Para os demais provedores, o total de interações que estes poderiam realizar com outros provedores foi determinado de forma aleatória dentro do intervalo de 1 a 512. O total de provedores que cada um desses interagiu também foi escolhido aleatoriamente de forma que no máximo cada provedor pode interagir com até 1/10 do total de provedores.

4.1. Resultados

A Figura 4 apresenta um histograma normalizado que ilustra o resultado das simulações, tendo no eixo X todos os cenários sobre os dois conjuntos de provedores candidatos a parceiros. As colunas representam o total de interações dividido entre os casos resultantes em sucesso e em insucesso. A normalização consistiu em adequar todos os cenários dentro da faixa de 0 a 1 no eixo y. Assim, é possível visualizar quais cenários apresentaram uma taxa percentual de sucessos maior.

O cenário 1 apresenta o caso sem qualquer modelo de reputação sendo que o compositor de processos interagiu todas as vezes com todos os provedores candidatos. Em ambos conjuntos, o total de interações realizadas para cenário 1 foi de 131.072 sendo que 50% das interações terminaram em sucesso e 50% em insucesso. O cenário serve como medida comparativa, determinando o total de interações possíveis diante do conjunto de entidades candidatas. Os resultados dos demais cenários são apresentados na Tabela 3.

Analisando os dados da Tabela 3 é possível concluir que o uso de sistemas de reputações permitiu, em média, um aumento de 30% das interações que resultaram em sucesso se comparado ao cenário 1. Apesar dos demais cenários apresentarem uma taxa de sucesso bem próximas, foi possível notar uma diferença no total de interações realizadas em cada cenário. Nos experimentos com o "conjunto de entidades 1", pode-se notar que o uso das opiniões providas pelo gerente apresentou melhores resultados quando

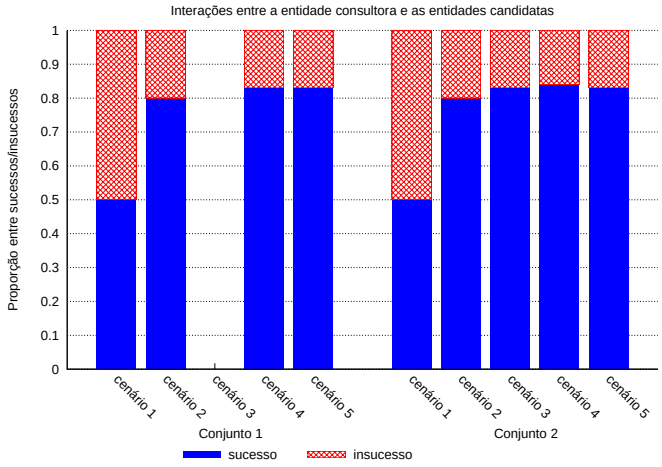


Figura 4. Resultado das interações entre o compositor de processos e os provedores candidatos

comparado com os cenários que só fizeram uso de experiências diretas ou mesmo consultando somente as entidades com quem se tinha relações de confiança estabelecidas. Para o "conjunto de entidades 2", é possível observar que apesar do cenário 5 apresentar uma taxa de sucesso semelhante aos cenários 3 e 4, teve-se um número maior de interações realizadas. No cenário 5 foram realizadas 43.433 interações que resultaram em sucesso, contra 24.011 e 41.131 dos cenários 3 e 4, respectivamente.

Tabela 3. Resultados do sistema de reputações

	Conjunto 1			Conjunto 2		
	Total de interações	Total de sucessos	Taxa de sucesso	Total de interações	Total de sucessos	Taxa de sucesso
Cenário 1	131.072	65.536	50%	131.072	65.536	50%
Cenário 2	47.386	37.908	80%	47.898	37.908	80%
Cenário 3	–	–	–	28.928	24.011	83%
Cenário 4	48.712	40.431	83%	49.434	41.131	83%
Cenário 5	48.712	40.431	83%	52.328	43.433	83%

Assim, é possível concluir que a combinação de diferentes bases de reputações apresenta uma taxa de sucesso elevada, mesmo diante de um maior número de interações. Nos cenários com bases isoladas, o número de interações foi menor, pois o sistema de reputação inferiu que as interações poderiam resultar em insucesso, desaconselhando assim a realização dessas interações.

5. Trabalhos relacionados

Em [Gray et al. 2003], [Wang and Vassileva 2003] e [Carbo et al. 2003] são apresentados sistemas de reputações que utilizam média ponderada para calcular a reputação de uma entidade qualquer. Cada proposta apresenta um uso particular para determinar os pesos. [Gray et al. 2003] baseia-se no número de entidades intermediárias existentes entre o requisitante e os provedores de opiniões em uma rede móvel *ad hoc*. [Wang and Vassileva 2003] utiliza a confiança existente entre o requisitante e os provedores de opinião e, também, técnicas de aprendizado por reforço para atualizar valores

de confiança. Em [Carbo et al. 2003], as opiniões recebidas são ponderadas com o fator chamado memória, o qual visa determinar se opiniões mais novas ou as mais velhas terão uma influência maior no cálculo da reputação.

Os trabalhos [Buchegger and Le Boudec 2004], [Whitby et al. 2005] e [Teacy et al. 2006] usam de maneira semelhante a distribuição beta para determinar a probabilidade de uma entidade vir a honrar a negociação. Este tipo de abordagem apresenta-se mais interessante do que aquelas que fazem uso de pesos, pois possuem uma fundamentação estatística. Estes trabalhos diferem entre si na forma como tratam a detecção de opiniões não confiáveis. Em [Whitby et al. 2005], as opiniões de provedores que se desviem de um limiar composto pela ampla maioria de opiniões, são descartadas. Em [Teacy et al. 2006], é comparado o histórico de opiniões fornecidas por um provedor com o que de fato foi observado nas interações com a entidade sobre quem este recebeu opiniões. Nesta última abordagem, se o provedor de opiniões fornecer de forma continuada opiniões parecidas, é assumido que o provedor é preciso, caso contrário, assume-se que as opiniões deste provedor são imprecisas e assim são descartadas.

O modelo proposto neste artigo também faz uso de média ponderada, porém os pesos utilizados são obtidos através de métodos estatísticos, com base nas experiências observadas pela entidade que está solicitando as opiniões. Como em [Teacy et al. 2006], as opiniões recebidas consideram o histórico do provedor de opiniões, permitindo que as opiniões de bons provedores prevaleçam sobre as opiniões de provedores maliciosos.

Porém, em [Teacy et al. 2006], para calcular o valor de esperado (veja Equação 3), os provedores de opiniões devem fornecer o número de interações que resultaram em sucesso e insucesso, com a entidade objeto do cálculo da confiança. Essa abordagem fere a privacidade dos provedores de opiniões e está factível ao ataque de descoberta de dados, onde uma entidade maliciosa pode ficar observando a evolução do provedor de opiniões com as demais entidades e assim utilizar dessas informações para benefício próprio. No modelo proposto, os provedores de opiniões só fornecem o valor esperado de forma que não se possa inferir sobre a quantidade total de casos com sucesso e insucesso.

O uso das bases de conhecimentos nos gerentes evita também uma das preocupações apresentadas em [Teacy et al. 2006], em que provedores de opiniões poderiam fornecer diferentes opiniões dependendo de quem as requisita. As bases de conhecimento no gerente só permitem incrementar os casos que resultam em sucesso e insucesso, mesmo sabendo que as entidades poderiam registrar opiniões diferentes do que realmente foi observado nas interações. Assim, uma vez que um provedor de opiniões registrou um caso de sucesso ou insucesso, essa informação estará disponível para qualquer requisitante e não poderá ser modificada.

6. Conclusões

O desenvolvimento dos Serviços *Web* como uma tecnologia modular e de interoperabilidade global, coloca-os como uma peça fundamental para a área de processos de negócios baseados em XML. Diante de um grande de número de provedores de serviços, a seleção de parceiros de negócios, de forma automática e sem a intervenção de usuários, é um desafio que vem despertando interesse da comunidade científica e da indústria. Neste artigo foi apresentado um modelo de confiança, aliado a um sistema de reputações, que visa o estabelecimento dinâmico da confiança entre parceiros de negócios, mesmo diante de

entidades que não possuam qualquer vínculo anterior.

Com a disponibilização das bases de conhecimento pelos gerentes das federações, evitou-se a principal preocupação apresentada pelos trabalhos relacionados. Ou seja, o sistema de reputação proposto apesar de permitir que uma entidade registre opiniões de forma maliciosa, este garante que as opiniões fornecidas serão concisas não importando quem as requisita, isto é, a base de reputações não pode ser manipulada de forma que apresente respostas diferentes para entidades distintas. O modelo proposto leva em consideração as experiências passadas para assim obter o valor da confiança sobre uma determinado provedor, sendo este um provedor de serviços ou um provedor de opiniões. Assim, entidades maliciosas (provedores de opiniões) serão facilmente identificados tendo suas opiniões ignoradas para o cálculo da confiança sobre as demais entidades do sistema distribuído.

Cada provedor no sistema possui uma base de conhecimento individual a qual agrupa experiências passadas e opiniões de provedores espalhados por diferentes domínios. Tal base é então usada para que se possa formar o valor da confiança sobre um provedor desconhecido qualquer e a interação com esse provedor só ocorrerá se o valor obtido atingir o limiar mínimo. Este tipo de abordagem permite ao modelo lidar com o problema do **conluio**, haja visto que a individualidade das bases de conhecimento sugere que tal ataque só terá êxito se este conseguir de certa forma cobrir a ampla maioria dos provedores de opiniões, tarefa a qual não é tão simples em sistemas de larga escala.

O modelo proposto também não está suscetível ao ataque denominado **traidor**. Em tal ataque, uma entidade poderia agir corretamente diversas vezes seguidas para situações onde o seu retorno fosse pequeno e então agir de forma maliciosa em uma situação onde seu retorno fosse maior. Por exemplo, um provedor de opiniões é consultado diversas vezes em algumas negociações de venda de CDs. Se este agisse de forma maliciosa nessas negociações, teria um retorno muito pequeno. Porém, este mesmo provedor de opiniões ao ser consultado pela primeira vez sobre uma negociação relacionada a venda de um automóvel, o alto valor envolvido nesta negociação poderia compensar seu comportamento malicioso. Neste trabalho o problema com o **traidor** pode ser minimizado através dos contextos de opiniões. O provedor do exemplo anterior teria uma ótima reputação no contexto de venda de CDs, entretanto no contexto de venda de carros sua reputação seria incerta. Isto faria com que a entidade requerente consultasse as outras bases de reputações que possui.

Referências

[Albert and Barabási 2002] Albert, R. and Barabási, A.-L. (2002). Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74:47.

[Bartel et al. 2002] Bartel, M., Boyer, J., and Fox, B. (2002). *XML-Signature Syntax and Processing*. W3C. `http://www.w3.org/TR/xmldsig-core`.

[Buchegger and Le Boudec 2004] Buchegger, S. and Le Boudec, J. (2004). A Robust Reputation System for Mobile Ad-hoc Networks. *Proceedings of P2PEcon, June*.

[Capkun et al. 2002] Capkun, S., Buttyan, L., and Hubaux, J.-P. (2002). Small worlds in security systems: an analysis of the PGP certificate graph. In *New Security Paradigms Workshop*, pages 28–35.

[Carbo et al. 2003] Carbo, J., Molina, J., and Davila, J. (2003). Trust management through fuzzy reputation. *International Journal of Cooperative Information Systems*, 12(1):135–155.

[Carminati et al. 2005] Carminati, B., Ferrari, E., and Hung, P. C. K. (2005). Web service composition: A security perspective. In *International Workshop on Challenges in Web Information Retrieval and Integration*, pages 248 –253.

[Charfi and Mezini 2005] Charfi, A. and Mezini, M. (2005). Using aspects for security engineering of web service compositions. In *IEEE International Conference on Web Services*, volume I, pages 59–66. IEEE.

[Grandison and Sloman 2000] Grandison, T. and Sloman, M. (2000). A Survey of Trust in Internet Applications. *IEEE Communications Surveys and Tutorials*, 3(4):2–16.

[Gray et al. 2003] Gray, E., Seigneur, J.-M., Chen, Y., and Jensen, C. D. (2003). Trust propagation in small worlds. In *International Conference on Trust Management*.

[Imamura et al. 2002] Imamura, T., Dillaway, B., and Simon, E. (2002). *XML Encryption Syntax and Processing*. W3C. `http://www.w3.org/TR/xmlenc-core`.

[Jain 1991] Jain, R. (1991). *The art of computer systems performance analysis*. Wiley.

[Khare and Rifkin 1998] Khare, R. and Rifkin, A. (1998). Trust management on the world wide web. *Computer Networks*, 30(1-7):651–653.

[Martin et al. 2004] Martin, D., Burstein, M., Hobbs, J., Lassila, O., Mcdermott, D., Mcilraith, S., and Narayanan, S. (2004). *OWL-S: Semantic Markup for Web Services*. W3C.

[Milgram 1967] Milgram, S. (1967). The small world problem. *Psychology Today*, 1:61.

[OASIS 2004a] OASIS (2004a). *Universal Description, Discovery and Integration v3.0.2*. Organization for the Advancement of Structured Information Standards (OASIS).

[OASIS 2004b] OASIS (2004b). *Web Services Security: SOAP Message Security 1.0*. OASIS.

[Sabater and Sierra 2001] Sabater, J. and Sierra, C. (2001). Regret: A reputation model for gregarious societies. *Workshop on Deception, Fraud and Trust in Agent Societies*, pages 61–69.

[Teacy et al. 2006] Teacy, W. T., Patel, J., Jennings, N. R., and Luck, M. (2006). Travos: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, 12(2):183–198.

[Wang and Vassileva 2003] Wang, Y. and Vassileva, J. (2003). Bayesian Network Trust Model in Peer-to-Peer Networks. *Workshop on Deception, Fraud and Trust in Agent Societies*, 7.

[Whitby et al. 2005] Whitby, A., Jøsang, A., and Indulska, J. (2005). Filtering out unfair ratings in bayesian reputation systems. *The Icfain Journal of Management Research*, 4(2):48–64.

[WS-Trust 2005] WS-Trust (2005). *Web Services Trust Language (WS-Trust)*.

[Wu et al. 2003] Wu, D., Parsia, B., Sirin, E., Hendler, J., and Nau, D. (2003). Automating DAML-S web services composition using SHOP2. In *International Semantic Web Conference*, Sanibel Island, Florida.