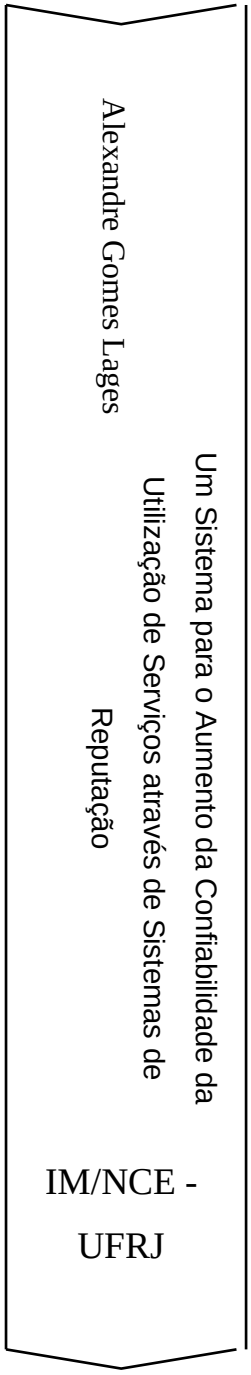
Instituto de Matemática / Núcleo de Computação Eletrônica
Universidade Federal do Rio de Janeiro

Alexandre Gomes Lages

Um Sistema para o Aumento da Confiabilidade da Utilização de Serviços através de Sistemas de Reputação

Rio de Janeiro

2007


Um Sistema para o Aumento da Confiabilidade da Utilização de Serviços através de Sistemas de Reputação
Alexandre Gomes Lages
IM/NCE - UFRJ

Alexandre Gomes Lages

Um Sistema para o Aumento da Confiabilidade da utilização de Serviços através de Sistemas de Reputação

Dissertação submetida ao corpo docente do Núcleo de Computação Eletrônica / Instituto de Matemática da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Ciências em Informática.

Rio de Janeiro

2007

FICHA CATALOGRÁFICA

LAGES, ALEXANDRE GOMES.

Um Sistema para o Aumento da Confiabilidade da utilização de Serviços através de Sistemas de Reputação, [Rio de Janeiro], 2007.

xii, 93 f., 29,7 cm (IM/NCE/UFRJ, Msc., Informática, 2007).

Dissertação (Mestrado) – Universidade Federal do Rio de Janeiro, IM/NCE.

1. Redes de Computadores 2. Sistemas de Reputação

3. Serviços Web 4. Redes Peer-to-Peer

Alexandre Gomes Lages

Um Sistema para o Aumento da Confiabilidade da Utilização de Serviços através de Sistemas de Reputação

Dissertação submetida ao corpo docente do Núcleo de Computação Eletrônica / Instituto de Matemática da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Ciências em Informática.

Aprovada por:

_____
Prof[a]. Luci Pirmez – Orientadora.
D. Sc., UFRJ.

_____
Prof[a]. Flávia Coimbra Delicato – Co-orientadora
D. Sc., UFRN.

_____
Prof. Luiz Fernando Rust da Costa Carmo**.**
Dr. UPS, UFRJ.

_____
Prof.Julius Leite.
Ph.D, UFF.

_____
Prof. Paulo de Figueiredo Pires.
D. Sc., UFRJ.

AGRADECIMENTOS

Aos meus pais, Henrique e Palmira (in memorian), que me ajudaram durante toda a minha vida.

Aos meus novos amigos que me ajudaram durante o período em que eu passei no NCE como bolsista e em seguida como aluno de mestrado: Nilson, Ana, Edson, André, e em especial ao Reinaldo pelas orientações fornecidas durante todo este período de tempo.

Ao professor Rust, pela oportunidade fornecida em trabalhar no Laboratório de Redes e Multimídia – Labnet.

Às minhas orientadoras Luci Pirmez e Flávia Delicato pela paciência, oportunidade e, sobretudo, pela confiança depositada.

Ao NCE/UFRJ pela infra-estrutura, fruto da dedicação de seus funcionários.

RESUMO

LAGES, Alexandre Gomes. Um Sistema para o Aumento da Confiabilidade da Utilização de Serviços através de Sistemas de Reputação. Rio de Janeiro, 2007. Dissertação (Mestrado em Informática) - Instituto de Matemática/Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

No ambiente da Web atual, a possibilidade de interação direta entre usuários, sem a presença de autoridades centrais para intermediar o acesso a um serviço, faz surgir à necessidade de sistemas eficientes que garantam a segurança das transações. Sistemas de Reputação, bastante usados em sítios de leilão eletrônico e redes Peer-to-Peer, têm como objetivo aumentar a confiabilidade e segurança das transações em nível de aplicação. Para realizar este objetivo, o sistema de reputação deve coletar, distribuir e agregar informações sobre o passado de transações dos participantes do sistema. Basicamente, os sistemas de reputação devem realizar duas funções: obter as informações sobre o passado de avaliações dos usuários e calcular um valor de reputação baseado nestas avaliações. A obtenção das informações dos usuários pode ser realizada através da utilização de um esquema centralizado ou distribuído, enquanto que a reputação é calculada através de um mecanismo de cálculo de reputação que pode utilizar métodos estatísticos, Sistemas Bayesianos, Lógica Nebulosa, entre outros. Este trabalho propõe um sistema de reputação orientado a serviço que utiliza Lógica Nebulosa para o cálculo dos valores de reputação, e que utiliza uma infra-estrutura Peer-to-Peer para a troca de informações sobre o passado de transações realizadas pelos usuários/peers. A característica inovadora da proposta é que, em um sistema orientado a serviço, os valores de reputação são associados não aos peers isoladamente, mas ao par peer-serviço. Esta solução permite que um peer possa ser confiável em acessar um serviço, enquanto que em outro não. A rede peer-to-Peer forneceu as primitivas para a troca de mensagens sobre as avaliações dos peers, enquanto que a adoção da Lógica Nebulosa foi devida à característica desta manipular dados imprecisos ou subjetivos das avaliações dos peers. Adicionalmente, o sistema de reputação adotou uma estrutura modular, podendo ser estendida para o uso em diversos cenários de aplicação. Inicialmente o sistema de reputação foi aplicado no aumento da segurança das estações em uma Rede Metropolitana Sem Fio (RMSF) com topologia Malha. Em seguida, de forma a aumentar a confiabilidade dos serviços fornecidos por provedores, o sistema de reputação proposto foi estendido para a inclusão de um cenário de comércio eletrônico baseado em Serviços Web. Esta extensão, a qual engloba o envio de mensagens de *probing* por peers monitores, garante que os parâmetros de QoS publicados pelos provedores estão de acordo com os valores medidos. Os resultados das simulações para ambos os cenários, RMSF e comércio eletrônico baseado em Serviços Web, demonstram que o sistema aumenta a segurança e a confiabilidade do uso os serviços.

ABSTRACT

LAGES, Alexandre Gomes. Um Sistema para o Aumento da Confiabilidade da Utilização de Serviços através de Sistemas de Reputação. Rio de Janeiro, 2007. Dissertação (Mestrado em Informática) - Instituto de Matemática/Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

In the current Web environment, users are able to directly interact with each other to exchange data and services, without intermediation of central authorities. Such scenario raises the need for efficient systems to assure the safety and confidence of transactions. The goal of reputation systems, which are widely used in electronic auction sites and Peer-to-Peer networks, is to increase the degree of reliability and security of transactions in application level. To accomplish this goal, the system must collect, distribute, and aggregate feedback information about participant's past behavior. Basically, reputation systems must carry out two main functions: the retrieving of users' past behavioral assessments and reputation values, and the calculating of users' final reputation values. The retrieving of users information may be accomplished by using a centralized or distributed scheme, while the final reputation value is calculated using a reputation computation engine that may employ an statistical method, Bayesian System, Fuzzy Logic, among others. This work proposes a reputation system that is service-oriented and makes use of Fuzzy Logic for the calculation of reputation values. It also employs a Peer-to-Peer infrastructure to distribute and exchange users/peers information, behavioral assessments and reputation values. The distinguishing feature of our proposal is that, in a service-oriented approach, the reputation values are not associated with the peers, but it is assigned to the pair peer-service. This solution augments the security of the whole system since a peer may be confident in executing a service while not trustable for using a different one. The Peer-to-Peer network as the underlying communication infrastructure plays an important role in our proposal once it enhances the reliability as long as the peers information are storage in many peers. In this way, at a given time, it is probable that there will be a set of peers to provide information to the requesting peers. The adoption of Fuzzy Logic technique was due to the imprecise or subjective nature of the behavioral peers assessments. This technique also reduced the complexity of the reputation calculation without loosing accuracy. In addition, our reputation system employs a modular structure, making it extensible for various scenarios of application. Our initial goal was to enhance the security of stations in a Wireless Metropolitan Area Network (WMAN) with a Mesh topology. Then, in order to increase the reliability of the services offered by providers, the proposed reputation system was extended to include a scenario of e-commerce based on Web Services. This extension, which encompasses monitoring peers employing probing messages, guarantees that the published QoS service parameter values are in accordance with the measured values. The simulation results for both scenarios, e-commerce and WMAN, show that our approach for reputation system effectively increases the security and reliability of the provided services.

Índices de Figuras

Lista de Tabelas

SUMÁRIO

Capítulo 1 Introdução

A evolução da Internet nos últimos anos possibilitou o surgimento de um cenário onde múltiplos usuários, incluindo empresas, pessoas, ou mesmo aplicações, podem interagir para a realização de troca de informações e dos mais variados serviços. Tais interações muitas vezes ocorrem diretamente entre pares anônimos ou desconhecidos, sem a intervenção ou o controle de uma autoridade central. Em tais cenários, é imprescindível a utilização de uma arquitetura e de mecanismos que garantam a segurança e a confiabilidade dos pares envolvidos nas comunicações.

As arquiteturas de segurança podem ser divididas em dois grupos: centralizadas ou distribuídas. Arquiteturas centralizadas apresentam problemas de escalabilidade e de não tolerância à falhas, enquanto que as distribuídas minimizam estes problemas, com o custo de serem mais complexas o seu desenvolvimento. O emprego de uma arquitetura distribuída em um cenário onde estações realizam transações eletrônicas de compra e venda de produtos sem a necessidade de uma autoridade central, representa uma alternativa preferível já que evita os problemas encontrados nas arquiteturas centralizadas.

Quanto aos mecanismos de segurança, como a utilização de criptografia, recursos de autenticação e assinatura das mensagens, estes são de extrema importância para o aumento da segurança das transações. Entretanto, são também necessários mecanismos complementares para o aumento da confiança quando da utilização de serviços entre os pares envolvidos, principalmente em nível de aplicação. Os sistemas de reputação podem ser utilizados com este objetivo.

Os sistemas de reputação [6] são empregados como um mecanismo para o aumento da confiabilidade do uso dos serviços em nível de aplicação. Estes sistemas se baseiam em interações prévias ocorridas entre os nós. Após um nó utilizar um serviço de outro, é atribuído ao nó um conceito referente à sua utilização deste serviço. De acordo com as interações passadas e com os conceitos que um nó possui, pode ser gerado um indicador sobre possíveis ações que o mesmo pode realizar no futuro. Um nó pode ter um valor de reputação para com diversos outros nós, com os quais interagiu, e a partir destes valores pode ser realizado o cálculo para a obtenção de um valor único, determinando a reputação deste nó. Na literatura são encontradas aplicações dos Sistemas de Reputação na escolha de peers confiáveis em redes Peer-to-Peer (P2P) [7, 8, 9], em sites de leilão eletrônico [10, 11], na escolha de estações confiáveis para o roteamento de fluxos de comunicação [12], entre outras.

Basicamente, os sistemas de reputação devem realizar duas funções: obter as informações sobre o passado de avaliações dos usuários e calcular um valor de reputação baseado nas avaliações. Para obter e distribuir os valores de avaliação sobre o passado dos usuários, pode ser utilizada uma rede P2P. As rede P2P fornecem as primitivas para a troca de mensagens entre os peers que podem ser usadas para transportar os valores de reputação.

Já para o cálculo do valor de reputação de um nó, podem ser utilizados métodos estatísticos, Sistemas Bayesianos[13, 14], Lógica Nebulosa (*Fuzzy Logic*) [7], entre outros. A capacidade de tratar dados lingüisticamente imprecisos, através da manipulação de valores imprecisos ou subjetivos, como a determinação de um grau de reputação baixo, médio ou muito alto, faz com que a Lógica Nebulosa seja uma alternativa bastante adequada para a realização de cálculos de valores de reputação. Adicionalmente, uma vez que a Lógica Nebulosa é baseada em um conjunto de variáveis e regras do tipo *Se* <premissa> *Então* <conclusão>, o seu uso pode acarretar uma menor complexidade computacional, quando comparada com outros modelos, como as Redes Neurais, por exemplo.

Sendo assim, os sistema de reputação fornecem um mecanismo para o aumento da confiabilidade no uso dos serviços. Entretanto, como a reputação é formada a partir da opinião de outros peers, um problema que pode afetar tais sistemas é a possibilidade da formação de **conluios**, que é a organização de um grupo de peers que visa aumentar ou diminuir a reputação de um ou vários peers da rede. Um outro problema que pode ocorrer ao utilizar uma infra-estrutura P2P para o armazenamento distribuído dos valores de reputação sobre os peers é a natureza dinâmica com que os peers entram e saem da rede. De forma a evitar que sejam perdidos valores de reputação sobre os peers, se faz necessário a manutenção de uma redundância no armazenamento das reputações sobre os mesmos.

A eficiência de um Sistema de Reputação depende do cenário em que este é adotado. Na maior parte dos Sistemas de Reputação existentes na literatura [7, 8, 9], o valor de reputação é atribuído ao próprio peer, e é usado para nortear suas interações com os outros peers. Não foi encontrado nenhum trabalho que apresenta um sistema de reputação cuja abordagem seja orientada a serviço fornecido em nível de aplicação, ou seja, onde a reputação atribuída refere-se ao par *peer-serviço*, utilizado em uma determinada aplicação, e não ao peer isoladamente.

Um cenário onde um Sistema de Reputação pode ser aplicado para o aumento da confiabilidade dos serviços disponíveis é em uma Rede Metropolitana Sem Fio (RMSF) com topologia Malha. Em tais redes, as estações podem interagir diretamente entre si, sem a

intermediação de uma unidade central, dessa forma comportando-se como peers em uma rede P2P. Em uma RMSF, uma Estação-Assinante pode trocar informações com outras Estações-Assinantes, bem como, entrar e sair da rede, de forma autônoma. Para garantir que as estações possam trocar informações, um sistema eficiente de reputação pode auxiliar os usuários a localizar parceiros confiáveis e trocar serviços de maneira segura.

Um outro cenário onde pode ser adotado um Sistema de Reputação é em um ambiente baseado em Serviços Web que utiliza uma Arquitetura Orientada a Serviços (SOA – *Service Oriented Architecture*). A utilização de uma SOA permite que sejam criadas aplicações compostas por serviços fracamente acoplados, aonde estes trocam informações através do envio de mensagens. Dessa forma, uma SOA depende fortemente de mecanismos de publicação e descoberta de serviços disponíveis. Atualmente os padrões Web para os mecanismos de publicação e descoberta de serviços são baseados nas descrições funcionais e sintáticas das características do serviço através de um arquivo utilizando a linguagem *Web Service Description Language* (WSDL) [15]. Além disso, os serviços de registro, como os serviços UDDI [16], não possuem a funcionalidade de permitir a descoberta e seleção de serviços baseados nas capacidades e comportamentos dos mesmos, uma vez que esses utilizam as informações disponíveis no arquivo WSDL, além da possibilidade do uso de informações sobre os provedores e a categorização dos mesmos. Portanto, vários trabalhos apontam a necessidade da inclusão de descrições semânticas de um serviço de maneira a melhorar o processo de descoberta e seleção de serviços em uma SOA [17, 18]. Principalmente é um consenso que os requisitos de QoS representam uma importante informação a ser incluída nas descrições dos serviços. Além das informações sobre os requisitos de QoS, também se faz necessário a adição mecanismos que avaliem se os requisitos de QoS publicados são realmente fornecidos. Em uma SOA, tais mecanismos são implementados através do uso de *Service Level Agreenments* (SLA) [19].

Tradicionalmente, uma SLA representa um acordo bilateral entre um provedor de serviço e os consumidores, na qual os parâmetros de QoS, como disponibilidade, *throughput* ou tempo de resposta, são precisamente definidos. Contratos eletrônicos baseados em SLAs somente funcionam propriamente se terceiros monitorarem os parâmetros de QoS acordados, de maneira a checar se a QoS efetivamente fornecida para os consumidores foi realizada como descreve a SLA. Para realizar a tarefa de monitoramento são utilizadas entidades de monitoramento que empregam mecanismos de *probing*, o qual consiste em enviar uma requisição de serviço para os provedores e armazenar os valores das métricas de QoS

efetivamente fornecidas. De maneira a não sobrecarregar de mensagens de *probing*, a freqüência de envio de *probes* deve ser ajustada para o menor valor possível, enquanto garante o valor das métricas de QoS fornecidas pelos provedores atualizadas. Portanto, existe uma questão a respeito da taxa de freqüência de envios de probes com o valor de QoS atualmente armazenado.

Entretanto, em ambientes SOA com alto grau de dinamismo, o uso de SLAs não é viável ou desejável devido ao seu custo inerente de estabelecimento. Um exemplo desse tipo de ambiente são os serviços Web públicos do tipo *pay per use*, como os disponibilizados no site Amazon.com [20]. Como nesse tipo de serviço toda a Web pode ser vista como potencial cliente, o estabelecimento de SLAs não é adequado devido, por exemplo, ao seu custo jurídico de estabelecimento. Assim, uma outra forma de SLA pode ser utilizada, onde o modelo bilateral é substituído por um modelo aberto no qual o provedor do serviço publica os parâmetros de QoS do serviço em um diretório público [21]. Os potenciais consumidores do serviço podem então, se basear na QoS publicada para selecionar os serviços de acordo com os requisitos de suas aplicações. Apesar do uso do mecanismo de publicação das métricas de QoS, estes ainda possuem o problema de fornecer garantias que as métricas de QoS (publicadas ou SLAs) serão respeitadas. Em um cenário real, contratos (como SLAs) podem ser violados e as métricas de QoS publicadas desrespeitadas. Este cenário implica que também se faz necessária a utilização de mecanismos que tratem da confiabilidade das métricas de QoS publicadas, indicando, por exemplo, o nível de confiança que um provedor possui em relação aos valores de QoS publicados/acordados.

1.1 Objetivos

A fim de incrementar a confiabilidade no uso de serviços em ambientes distribuídos, este trabalho propõe a utilização de um Sistema de Reputação com uma abordagem orientada a serviço. Foram adotados como cenários de aplicação do sistema proposto uma Rede Metropolitana Sem Fio com Topologia Malha e um ambiente de Serviços Web que utiliza uma Arquitetura Orientada a Serviços, pois o sucesso de uso de tais cenários depende fortemente de um sistema eficiente de segurança. Para o Sistema de Reputação proposto são apresentados: (i) o mecanismo de troca de mensagens para a descoberta da reputação atribuída ao par *peer-serviço*; (ii) a forma como é realizado o cálculo da reputação do mesmo; (iii) o mecanismo para minimizar a formação de conluios; e (iv) os resultados das simulações realizadas com o protótipo implementado nos dois cenários de utilização.

Para a troca de mensagens para a descoberta dos valores de reputação atribuídos ao par *peer-serviço* foi implementada uma rede Peer-to-Peer sobreposta à infra-estrutura do cenário de aplicação utilizado. Além da troca de mensagens, a rede Peer-to-Peer fornece as primitivas para a instalação de peers com a responsabilidade de armazenar os valores de reputação.

O cálculo da reputação de um par peer-serviço é realizado através da utilização de um sistema nebuloso, e no Sistema de Reputação proposto são calculados dois valores de reputação: uma Reputação Individual e uma Reputação Agregada. A Reputação Individual é calculada utilizando somente as avaliações fornecidas por peers conhecidos, isto é, por peers com os quais o peer já interagiu previamente, enquanto que a Reputação Agregada é calculada utilizando todas as avaliações fornecidas pelos peers da rede. Os peers com os quais um peer já interagiu, seja como cliente ou fornecedor de um serviço, formam o que é denominado de Rede de Relacionamento. As avaliações fornecidas por estes peers representam um valor mais confiável, uma vez que são peers com o qual o peer já possui um valor de relacionamento, e são utilizadas para o cálculo da Reputação Individual. Uma vez que a Reputação Individual é calculada utilizando somente valores de avaliação obtidos dos peers com o qual já possui um valor de relacionamento, esta não apresenta o problema do conluio, entretanto, peers novos ou peers que tenham acessado ou fornecido poucos serviços podem não possuir valores de avaliação para o cálculo da Reputação Individual.

Já a Reputação Agregada é calculada utilizando todos os valores de avaliação disponíveis sobre um peer, minimizando a probabilidade de não haver avaliações disponíveis para o cálculo. Entretanto, ao utilizar todas as avaliações sobre um peer, pode ocorrer o problema do conluio no cálculo da Reputação Agregada. De forma a minimizar o problema do conluio no cálculo da Reputação Agregada é utilizada uma distribuição de freqüências para o descarte de avaliações fornecidas sem critério (ou propositalmente maliciosas). Caso a avaliação esteja dentro do padrão de distribuição de freqüência atribuídos ao par peer-serviço, o processo de atualização da reputação é realizado através da aplicação de um filtro, baseado na reputação e no relacionamento que atribuiu à nova avaliação.

De forma a incorporar o Sistema de Reputação proposto a um ambiente de Serviços Web que utiliza uma Arquitetura Orientada a Serviços, este trabalho apresenta o SATYA, uma extensão do Sistema de Reputação proposto desenvolvido com o objetivo de aumentar a confiança do uso dos serviços fornecidos por provedores. A confiança é representada no SATYA através do uso de valores de reputação, que são atribuídos a cada métrica de QoS que um provedor publica.

O SATYA atribui e gerencia os valores de reputação dos provedores de serviço calculados a partir das (i) avaliações fornecidas pelos clientes dos serviços e (ii) dos valores objetivos obtidos pela entidade de monitoramento. Os valores objetivos e as avaliações subjetivas são comparados com o objetivo de: (i) validar as avaliações subjetivas; (ii) minimizar o grau de subjetividade dos valores de reputação calculados; e (iii) descobrir as preferências dos clientes e provedores em termos das métricas de QoS. De forma a não impactar a infra-estrutura de rede com as mensagens de *probing*, o SATYA adota um mecanismo que adapta dinamicamente a taxa de freqüência de *probing* de maneira a refletir o estado corrente de fornecimento de serviços por parte do provedor. Este mecanismo representa uma característica única presente no SATYA em comparação com outros mecanismos existentes que utilizam uma taxa de freqüência fixa. Utilizando uma taxa de freqüência de *probing* dinâmica apresenta a vantagem de aumentar a escalabilidade do sistema proposto em termos do número de mensagens de *probing* necessárias para manter atualizado as métricas de QoS que um provedor fornece.

Em relação aos valores de preferência calculados pelo SATYA, estes são usados como mecanismo de incentivo, para estimular clientes a fornecerem avaliações, e fornecer para os clientes dos serviços um mecanismo que restringe a busca por provedores que pertençam ao mesmo grupo de preferência que o cliente. Ao fornecer aos clientes de um grupo de preferência a capacidade de escolherem provedores que fornecem um “melhor serviço” na mesma métrica de preferência do grupo, pode resultar em uma maior satisfação no uso dos serviços por parte dos clientes. Baseados na possibilidade de obterem um “melhor serviço” ao utilizarem os provedores que pertencem ao mesmo grupo de preferência, os clientes possuem o incentivo de fornecer as avaliações para então ser calculado os grupos de preferência.

1.2. Organização

O restante deste trabalho está estruturado em cinco capítulos. No segundo capítulo, são apresentados os conceitos básicos para a compreensão deste trabalho. Serão descritas funcionalidades que um Sistema de Reputação possui, assim como, os trabalhos relacionados na área e os conceitos necessários referente a utilização da Lógica Nebulosa. O terceiro capítulo apresenta a descrição detalhada do Sistema de Reputação proposto, descrevendo o mecanismo de troca de mensagens dos valores de reputação, a forma de cálculo utilizando Lógica Nebulosa e os mecanismos para minimizar o problema do conluio. No capítulo seguinte é detalhada a extensão do Sistema de Reputação proposto SATYA aplicado a um cenário de Serviços Web que utiliza uma Arquitetura Orientada a Serviços. No quinto

capítulo, são descritos as simulações realizadas, sendo então analisados os resultados obtidos. Por fim, no sexto capítulo são apresentadas as conclusões e os trabalhos futuros.

Capítulo 2 Conceitos Básicos

Este capítulo tem por objetivo apresentar os conceitos básicos que nortearam o desenvolvimento do sistema de reputação proposto.

Assim, são apresentados na Seção 2.1 os conceitos de confiança e reputação. A Seção 2.2 relaciona os principais aspectos dos sistemas de reputação, descrevendo as funcionalidades, arquiteturas e principais dificuldades de se implantar tais sistemas. A Seção 2.3 trata das Redes Peer-to-Peer, tipo de rede que o sistema de reputação proposto utiliza para a troca de valores de reputação dos usuários do sistema (peers). A Seção 2.4 descreve sucintamente os Serviços Web, pois os testes de validação do sistema de reputação proposto foram realizados considerando aplicações baseadas em tais serviços. A Seção 2.5 apresenta os principais conceitos da Lógica Nebulosa que foi utilizada no presente trabalho para o cálculo da reputação. Na Seção 2.6, são apresentados diversos trabalhos relacionados a presente proposta. Por fim, a Seção 2.7 finaliza este capítulo tecendo algumas conclusões.

2.1 Reputação e Confiança na Utilização de Serviços

Os conceitos de confiança e reputação podem ser utilizados na concepção de mecanismos de suporte a aplicações para que estas possam acessar e fornecer serviços de forma segura. Em ambientes onde clientes e provedores de serviços nunca interagiram previamente, a utilização de mecanismos baseados nesses conceitos podem fornecer uma avaliação preliminar de quais ações podem ser executadas de forma mais segura pelos clientes no acesso aos serviços dos provedores.

A confiança é um conceito abrangente que engloba diversas definições [22]. Entretanto, no contexto do presente trabalho, foi adotado aquela apresentada em [22]. Nesta definição, a confiança é uma medida que quantifica a disposição de uma entidade em depender, em determinada situação e com relativa segurança, de algo ou alguém, assumindo que conseqüências negativas possam ocorrer.

Neste contexto, a confiança incorpora os conceitos de dependência e risco. A dependência é aquela entre pares, ou seja, de clientes em relação a provedores e vice-versa. O risco se refere à probabilidade de ocorrerem conseqüências negativas quando clientes acessam serviços nos provedores ou quando estes prestam serviços aos clientes. O risco aumenta, por exemplo, quando o valor envolvido em uma transação é alto e a probabilidade de ocorrer uma falha não pode ser desconsiderada.

Já o conceito de reputação está atrelado com a confiabilidade, uma vez que a reputação é formada por informações fornecidas por terceiros. O presente trabalho segue a definição

proposta em [23], na qual estabelece que a reputação é um valor resultante daquilo que é atribuído a alguém ou algo. Esta definição é especialmente talhada para ambientes de redes onde é relativamente simples disponibilizar informações fornecidas por terceiros sobre interações passadas realizadas por uma determinada entidade. Neste caso, o valor de reputação, computado a partir dessas interações passadas, fornece a terceiros uma avaliação preliminar sobre a confiabilidade da referida entidade em fornecer ou acessar serviços.

Utilizando as definições de confiança e reputação adotadas no presente trabalho, pode-se claramente diferenciar os conceitos de reputação e confiança analisando as duas sentenças a seguir [23]:

1. *"Eu confio em você apesar da sua péssima reputação"*
2. *"Eu confio em você por causa da sua boa reputação"*

Assumindo que as duas sentenças compreendem o acesso ou o fornecimento de um mesmo serviço, a primeira sentença representa a utilização de uma informação privilegiada a respeito da entidade a ser avaliada, que pode ter sido obtida através da interação diretamente realizada entre os pares, por exemplo. Já a segunda sentença representa a utilização de informações fornecida por terceiros para a avaliação da entidade, podendo ou não ter sido utilizada uma informação privilegiada no cálculo da reputação.

2.2 Sistemas de Reputação

Os sistemas de reputação [6] possuem a função de coletar, distribuir e agregar os diversos valores de avaliação sobre os usos de serviços que uma entidade realizou no passado. Baseado nestes valores de avaliação é calculado um valor de reputação da entidade em questão. Assim, os mecanismos de decisão podem se utilizar desse valor de reputação para decidirem se um novo serviço será ou não fornecido para a mesma entidade. Outra hipótese seria fornecer o serviço com restrições, estabelecendo que tipos de ações que serão permitidas na execução do serviço.

Segundo [6], os sistemas de reputação devem possuir três propriedades:

1. As entidades pertencentes ao sistema devem permanecer longos períodos de tempo conectados a rede;
2. As avaliações sobre as interações realizadas pelas entidades devem estar distribuídas;
3. As avaliações sobre o passado das interações realizadas devem guiar as decisões futuras de novas interações;

A razão das entidades precisarem estar longos períodos de tempo conectados advém do fato de que os sistemas de reputação são dependentes de informações históricas de avaliação do comportamento das entidades pertencentes ao sistema. Para curtos períodos de tempo de conexão, existe uma maior probabilidade de uma determinada entidade, que esteja, por exemplo, acessando um serviço, possuir nenhum histórico de avaliação, inviabilizando o cálculo de sua reputação. Nestes casos, são atribuídos empiricamente valores iniciais de reputação (muito baixos), que são menos confiáveis do que aqueles calculados a partir de valores históricos de avaliação.

A necessidade das informações estarem distribuídas reside em se evitar os problemas inerentes aos sistemas centralizados, tais como um único ponto de falha, entre outros. Uma estratégia de distribuição de informações de avaliação bastante explorada é a utilização de redes Peer-to-Peer (P2P) sobreposta à infra-estrutura de rede utilizada. As redes P2P fornecem as primitivas para a troca de mensagens entre os peers que podem ser usadas para transportar os valores de reputação. Essas mensagens podem ser distribuídas para todos os peers ou somente para parte deles, denominados Super-Nós.

A terceira propriedade determina o uso dos valores de reputação na decisão do fornecimento de futuros serviços para as entidades envolvidas no sistema.

Como as avaliações são vitais aos sistemas de reputação e, por conseguinte, para assegurar ou, no mínimo, aumentar o número de avaliações, mecanismos de incentivos de avaliação do uso de serviços devem ser utilizados. Em [24] e [25] são identificadas três classes de mecanismo de incentivo: baseados em comércio, baseados em reciprocidade e os baseados na generosidade.

O incentivo baseado em comércio caracteriza-se por oferecer alguma vantagem ou compensação àquelas entidades que se disponham a fornecer avaliações de outras entidades. As vantagens incluem esquemas de micro-pagamento (remuneração do peer que fornece o recurso) assim como de troca de recursos. Um outro tipo de compensação é o fornecimento, por parte do próprio sistema de reputação, de benefícios para as entidades que forneçam avaliações, como a utilização de um recurso de uma entidade com baixa sobrecarga, por exemplo.

Nos mecanismos de incentivo baseados em reciprocidade, um usuário A fornece um recurso para um usuário B baseado nos recursos que o usuário B já forneceu para o usuário A, ou para outros usuários do sistema. Cada usuário mantém uma base de informações contendo as ações realizadas por outros usuários e usa estas informações para fornecer ou não um

recurso. O conjunto de informações sobre o passado de ações de um usuário representa então a reputação deste.

Já os mecanismos de incentivo baseado em generosidade representam uma categoria onde os usuários decidem se contribuirão ou não com o sistema baseados nas contribuições fornecidas por outros usuários. Resultados a partir da utilização de um modelo em [26] demonstram que quando a generosidade empregada pelos usuários no sistema está abaixo de certo limiar, o sistema entra em colapso por causa da grande quantidade de usuários egoístas.

2.2.1 Sistemas de Reputação Centralizados X Sistemas de Reputação Distribuídos

Quanto aos esquemas de armazenamento e distribuição dos valores de reputação calculados, os sistemas de reputação podem ser de dois tipos: centralizado ou distribuído. Nos sistemas de reputação centralizados, existe a presença de uma entidade central que coleta os valores de avaliação sobre as transações realizadas entre as entidades e distribui os valores de reputação baseados nas requisições dos mesmos. Como exemplo, os sítios Mercado Livre e Ebay [10, 11] utilizam um sistema de reputação centralizado de forma a fornecer valores de confiabilidade sobre as transações eletrônicas realizadas pelos usuários. Esses sistemas de reputação centralizados são mais simples de serem desenvolvidos, entretanto tais sistemas possuem severos problemas de escalabilidade e de apresentarem um ponto único de falha no sistema, que é o elemento central de armazenamento das avaliações das entidades.

De forma a contornar os problemas apresentados pelos sistemas de reputação centralizados, os distribuídos armazenam as informações de reputação nas próprias entidades (nós da rede, ou, no caso de redes P2P, os peers). Para determinada entidade obter o valor de reputação de uma outra entidade, aquela entidade envia requisições para diversos nós. Uma vez de posse dessas avaliações a entidade requisitante procede ao cálculo do valor de reputação.

Apesar dos sistemas de reputação distribuídos minimizarem os problemas encontrados nos sistemas de reputação centralizados, tais sistemas são mais complexos de ser construir. Por exemplo, no desenvolvimento do protocolo de comunicação para a troca de mensagens de avaliação, deve se ter o cuidado de considerar, entre outros aspectos, as confiabilidades dos nós (peers) que fornecem as avaliações.

Na literatura, são encontrados trabalhos que fazem uso de redes P2P [7, 8, 25] na concepção de sistemas de reputação distribuídos. As redes P2P, devido a sua natureza, possuem um conjunto de problemas de segurança, como grande facilidade de propagação de vírus e de outros programas maliciosos, entre outros. Sistemas de reputação podem então ser

aplicados em redes P2P para que peers busquem e selecionem peers confiáveis que possam fornecer recursos e, também, para que peers fornecedores de serviços avaliem previamente a reputação dos peers solicitantes de recursos.

2.2.2 Métodos para o Cálculo da Reputação

Independentes da arquitetura utilizada no sistema de reputação ser centralizada ou distribuída, a literatura apresenta diversos métodos para o cálculo da reputação final de uma entidade [23]. A forma mais simples de cálculo da reputação é a soma de todos os valores de avaliação obtidos dos nós da rede. Este método pode ser melhorado através do cálculo da média simples ou média ponderada dos valores de avaliação.

Além dos métodos de soma e média que podem ser utilizados, diferentes trabalhos apresentam métodos teóricos para o cálculo da reputação, como a utilização de Sistemas Bayesianos [13, 14], Modelos Discretos de Cálculo da Confiança (*Discrete Trust Models*) [27], Lógica Nebulosa [7], entre outros [23].

O presente trabalho adota a Lógica Nebulosa para o cálculo da reputação. A escolha deste método se justifica pelo fato de que a Lógica Nebulosa é indicada para manipular dados de características imprecisas ou subjetivas, como é o caso dos valores de avaliação e reputação utilizados nos sistemas de reputação. As características [28] que a Lógica Nebulosa possui são: (i) construir, entender, manter e testar modelos mais facilmente; (ii) desenvolver protótipos em um espaço curto de tempo; (iii) conceber sistemas mais robustos; (iv) manipular informações imprecisas, através da utilização de um conjunto de regras que conseguem expressar as imprecisões e aproximações dos métodos.

2.2.3 Problemas existentes com o uso de um Sistema de Reputação

Fundamentalmente, os problemas enfrentados por um sistema de reputação são classificados em três categorias [29]: (i) como tratar a entrada de novas entidades no sistema de reputação, (ii) como minimizar o problema de um grupo de entidades que fornecem deliberadamente valores de avaliação com o intuito de aumentar ou diminuir a reputação de uma entidade específica, problema conhecido como conluio, e (iii) como evitar que uma entidade, que durante certo período tempo acumulou uma reputação alta, efetue um ataque contra uma outra entidade.

O primeiro problema é conhecido como *whitewashing* que ocorre em sistemas onde as entidades podem facilmente mudar seus próprios identificadores e entrar novamente no sistema com um novo identificador como se fossem novas entidades e formar uma reputação. Se o sistema adotar uma política permissiva para o fornecimento de recursos, as entidades

podem trocar de identidade de tempos em tempos para criarem novas reputações. A possibilidade de uma entidade trocar facilmente de identificador pode levar o sistema ao colapso [25].

O problema de conluio em sistemas de reputação ocorre quando um grupo de peers está comprometido em aumentar ou diminuir a reputação de um determinado peer. Este problema apresenta-se de forma inevitável, uma vez que os sistemas de reputação utilizam as informações fornecidas muitas vezes por entidades desconhecidas, isto é, com as quais nunca interagiu.

O terceiro tipo de problema é conhecido como ataque da entidade traidora [29] e ocorre quando uma entidade utiliza de forma correta os serviços oferecidos na rede durante certo período de tempo, e após a formação de uma reputação alta, esta entidade efetua um ataque. Este tipo de ataque é extremamente difícil de ser detectado, e o mecanismo que vem sendo mais comumente utilizado para reduzir a freqüência de sua ocorrência é a utilização do passado histórico recente da entidade [29].

2.3 Redes Peer-to-Peer

As redes Peer-to-Peer (P2P) são redes virtuais que funcionam na Internet com o objetivo de compartilhar recursos entre os participantes, sendo que, por princípio, não há diferenciação entre os participantes [30]. Os participantes de uma rede P2P são denominados de peers que têm a capacidade de trocar informações entre si como arquivos de música, dados, vídeos, ciclos de CPU, armazenamento e largura de banda sem a necessidade de uma autoridade central para intermediar a troca [29].

Quanto à forma de como os peers se estruturam para a troca de informações, os peers são organizados formando uma Rede de Sobreposição (*Overlay Network*), ou seja, os peers são conectados logicamente por protocolos em nível de aplicação, que por sua vez estão sobrepostos aos protocolos de transporte. Dessa maneira, pode-se abstratamente considerar que uma rede virtual parcialmente conectada fica incorporada sobre a infra-estrutura de rede. Essa rede virtual é utilizada para a troca de mensagens que, no contexto do presente trabalho, transporta os valores de reputação.

A organização da rede de sobreposição pode ser realizada de duas maneiras: não-estruturada e estruturada. Uma organização não-estruturada da rede de sobreposição implica que a entrada e conexão de um novo peer são realizadas de forma randômica, isto é, não existe a obrigação do novo peer estabelecer uma conexão com um peer específico pertencente à rede de sobreposição, podendo ser escolhido qualquer peer da rede de sobreposição. A

procura por recursos na rede é realizada geralmente através do processo de inundação, sendo que novos mecanismos vêm sendo propostos para evitar este processo [29].

Já em uma organização estruturada da rede de sobreposição, a organização dos peers é realizada através de um esquema de alocação de chaves e identificadores, associando um determinado recurso ou serviço a um peer específico dentro da rede de sobreposição. Os peers pertencentes à rede de sobreposição estruturada armazenam tabelas de roteamento contendo as chaves e os identificadores, de forma que os recursos ou serviços podem ser encontrados através de um número pequeno de saltos.

2.4 Arquiteturas Orientadas a Serviço baseadas em Serviços Web

Uma Arquitetura Orientada a Serviços (*Service Oriented Architecture – SOA*) [21] representa a utilização de um modelo em que a funcionalidade fornecida por um conjunto de serviços são compostos de forma a criação de uma aplicação. A utilização deste modelo tem como objetivos: (i) a possibilidade de reuso de diversos serviços implementados; (ii) eficiência na criação de novas aplicações através da composição de serviços existentes com a criação de novos; e (iii) baixo acoplamento entre os serviços compostos, de forma que estes podem ser testados e avaliados independemente.

Em uma SOA, a utilização de Serviços Web permite que sejam criadas aplicações baseadas na Internet independentes de plataforma ou linguagem de programação. Através da utilização de padrões como o SOAP [31], registros UDDI [16], e da descrição dos serviços utilizando WSDL [15], podem ser criados Serviços Web que podem interagir com outros Serviços Web. A interoperabilidade advém do fato da utilização destes padrões.

A Figura 1 mostra o funcionamento da arquitetura de um Serviço Web. Quando um provedor deseja fornecer um serviço para os clientes, esse publica um documento WSDL descrevendo as propriedades sintáticas do serviço fornecido em um registro presente no Agente de Serviços. O Agente de Serviços tem a funcionalidade de armazenar uma descrição sobre a localização onde os arquivos WSDL sobre os serviços fornecidos pelos provedores podem ser recuperados, e fornecer estes documentos para clientes dos serviços quanto estes enviam requisições. Um cliente ao efetuar uma busca por um serviço em um Agente de Serviços e receber o documento WSDL, esse terá o endereço e outras características do serviço, como as interfaces, para poder requisitar o serviço do provedor.

Figura 1 – Arquitetura de Serviços Web

Dessa forma, em uma SOA que utiliza Serviços Web para a criação de aplicações, são necessários mecanismos para a publicação e descoberta de serviços que retornem informações confiáveis a respeito dos provedores de serviços. De forma a prover uma maior confiabilidade no uso das informações publicadas pelos provedores, o uso de um Sistema de Reputação pode ser empregado de forma a avaliar os provedores quanto as informações a respeito do serviço publicadas no Agente de Serviços.

2.5 Lógica Nebulosa

A Lógica Nebulosa compreende a modelagem de forma aproximada ao comportamento do raciocínio humano, através do desenvolvimento de sistemas computacionais que tratam de problemas complexos envolvendo dados imprecisos ou subjetivos. O uso da Lógica Nebulosa permite que sejam tratadas informações imprecisas através da utilização de um conjunto de regras de inferência.

A teoria da Lógica Nebulosa foi introduzida em 1965 por Lotfi Zadeh [32], com o objetivo de fornecer um tratamento matemático a certos termos lingüísticos subjetivos como “próximo”, “em torno de”, entre outros. Na Lógica Tradicional as variáveis podem receber valores do tipo verdadeiro ou falso, zero ou um. Já na Lógica Nebulosa, as variáveis denominadas de variáveis lingüísticas (ou variáveis nebulosas) são representadas de forma contínua. Por exemplo, a criação da variável lingüística altura, representando a altura de uma pessoa, não é representada por um valor exato, mas por um intervalo de valores juntamente com a sua função de inclusão.

Dessa forma, a definição de uma variável nebulosa é realizada através de conjuntos, onde cada um representa um dos intervalos de valores da variável nebulosa, os quais são associados a regras semânticas. A avaliação de uma dada proposição em um conjunto nebuloso pode resultar em qualquer valor real compreendido no intervalo [0,1]. Diz-se, então, que existe um grau de inclusão (pertinência) de cada elemento em um dado conjunto. No exemplo de um conjunto de pessoas altas não existe uma fronteira bem definida para decidir

se uma determinada pessoa pertence ou não a este conjunto, de forma que podem ocorrer sobreposições de conjuntos.

Os conjuntos nebulosos permitem então definir critérios e graus de inclusão que incorporam essas incertezas. O grau de inclusão é definido pela função de inclusão, a qual representa o grau de pertinência do elemento em um conjunto nebuloso. Portanto, uma vez identificados os conjuntos nebulosos, a próxima tarefa é descobrir a melhor forma de determinar a função de inclusão. Na literatura encontram-se várias famílias de funções de pertinência (inclusão) parametrizadas, sendo que as funções triangulares e trapezoidais são as mais comumente utilizadas.

A Figura 2 mostra dois exemplos de funções de pertinência. A Figura 2 (a) apresenta a função triangular que é utilizada quando existe apenas um único elemento de um conjunto cujo grau de inclusão é um (1). Já a Figura 2 (b) mostra a função trapezoidal, que é utilizada quando existe um intervalo de elementos de um conjunto cujos graus de inclusão são iguais a um (1).

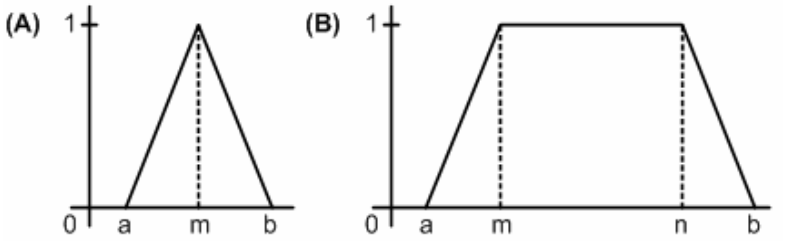


Figura 2 – Funções de Pertinência: (a) Triangulares (b) Trapezoidais

A criação de uma variável lingüística é definida através de uma quádrupla (X, R(X), U, M), onde X representa o nome da variável, R(X) é o conjunto de valores lingüísticos de X, isto é, os rótulos da variável lingüística X, U é o Universo de Discurso, representando os valores que a variável lingüística X pode assumir, e M são as regras semânticas que indicam o significado de cada rótulo em R(X).

Concluída a fase de definição das variáveis nebulosas com os seus conjuntos nebulosos, a criação de um sistema nebuloso é realizada através da criação de uma base de regras, formada por um grupo de condições do tipo **Se** <premissa> **Então** <conclusão>, que determinam as ações de controle em função das várias faixas de valores que as variáveis de estado do problema podem assumir. A Figura 3 representa os componentes de um sistema nebuloso.

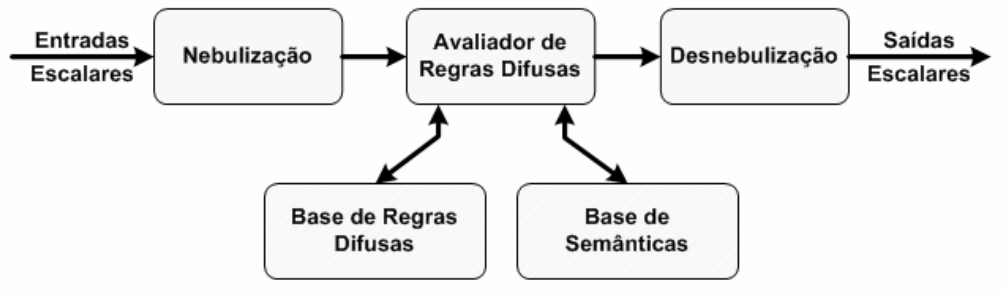


Figura 3 – Sistema Nebuloso

Conforme mostra a Figura 3, as entradas e saídas são valores escalares. O processo de Nebulização mapeia as entradas escalares ou *crisp* de entrada e as converte em variáveis nebulosas definidas pelos conjuntos nebulosos na Base de Semântica. Em seguida, as entradas convertidas em variáveis nebulosas são submetidas ao Avaliador de Regras Difusas que é o responsável pela aplicação das regras difusas armazenadas na Base de Regras Difusas, obtendo-se as saídas nebulosas. Por fim, as variáveis nebulosas de saída passam pelo processo de Desnebulização, onde são novamente transformadas em valores escalares.

2.6 Trabalhos Relacionados

O desenvolvimento do sistema de reputação do presente trabalho foi feito em duas etapas: (i) primeiramente foi desenvolvido o módulo que realiza o cálculo da reputação dos peers, e em seguida, (ii) este módulo foi estendido com a adição de novos módulos para a sua utilização em um ambiente de Serviços Web que utiliza uma Arquitetura Orientada a Serviços. Na Seção 2.6.1 estão apresentados os trabalhos relacionados ao cálculo da reputação, enquanto que a Seção 2.6.2 descreve os trabalhos relacionados ao uso da reputação em um ambiente de orientado a serviços.

2.6.1 Trabalhos relacionados no cálculo da Reputação

Atualmente os sistemas de reputação mais utilizados estão na área de comércio eletrônico [10, 11]. O sítio Mercado Livre [10] utiliza um processo de cálculo de reputação denominado Processo de Qualificação, que avalia os usuários após a compra ou venda de produtos no sítio. Neste processo, é utilizada uma arquitetura centralizada no armazenamento das reputações (no sítio é utilizado o termo Qualificações) dos usuários que são disponibilizadas para o público em geral. Entretanto, esse sistema apresenta uma deficiência no cálculo da reputação dos usuários, pois não é levada em conta a reputação do usuário que está atribuindo uma nova avaliação de compra ou venda de uma mercadoria. Outra desvantagem desse sistema de cálculo é que a pontuação atribuída por um usuário novo

possui o mesmo peso de um usuário que já realizou diversas operações de compra e venda e, portanto, já possui um histórico de relacionamento no sistema.

Em [33] é apresentado um sistema de reputação que utiliza uma arquitetura distribuída para armazenar os valores de reputação dos peers, com a característica de manter anônimos os peers responsáveis pelo armazenamento, impedindo ataques como a formação de conluios. Entretanto, para garantir o anonimato dos peers é utilizado um nó especial chamado *Bootstrap* para a escolha dos peers que armazenarão a reputação de um novo peer que entra na rede. Caso este nó seja comprometido, através da descoberta do algoritmo utilizado para escolha do nó, os peers perderão a características de serem anônimos. Um outro problema não relacionado está na utilização de um processo de inundação de mensagens na rede para a descoberta de um valor de reputação.

O trabalho apresentado em [8] utiliza o algoritmo EigenTrust que calcula a reputação de um peer utilizando o histórico de transações realizadas por ele. Para minimizar o tempo de busca dos valores de reputação dos peers é utilizado um algoritmo de Tabela Hash Distribuída. A reputação de um peer é calculada através de uma média ponderada com base nos valores de reputação fornecidos pelos peers com os quais o peer interagiu. Os pesos utilizados para o cálculo da média ponderada são os valores de reputação de cada peer que forneceu a reputação.

Já o trabalho descrito em [7] é o que apresenta maior semelhança com a presente proposta de cálculo de reputação. Neste trabalho é apresentado o FuzzyTrust que é um sistema de reputação que utiliza Lógica Nebulosa e foi baseado em um estudo sobre as transações de comércio eletrônico no site Ebay [11]. No FuzzyTrust são calculados dois valores de reputação: local e global. A reputação local emprega um sistema nebuloso para o cálculo da reputação de um peer. A reputação global agrega os valores de reputação local calculados individualmente pelos peers utilizando o sistema nebuloso e retorna um valor de reputação global para cada peer. Entretanto, o FuzzyTrust não adota a abordagem orientada a serviços, como na presente proposta, atribuindo os valores de reputação aos peers isoladamente. Além disso, não é tratada a possibilidade de acesso de um peer a um serviço, mesmo este tendo uma baixa reputação. O FuzzyTrust apresenta o problema do conluio ao utilizar todos os valores de reputação que um peer possui para o cálculo da reputação global. Além disso, não são apresentadas contramedidas para este problema.

Com o objetivo de diminuir o consumo de banda na rede para a obtenção do valor de reputação de um peer, o trabalho em [9] realiza a comparação de dois métodos para o cálculo

da reputação: (i) utilização de todos os valores de reputação que um peer possui distribuídos em todos os peers com os quais já interagiu, ou (ii) utilização de métodos estatísticos em somente uma parte da rede. A utilização de todos os valores de reputação apresenta uma forma de cálculo mais exato, e para isto é utilizado um grafo representando as interações ocorridas entres os peers. Percorrendo as arestas deste grafo podem ser gerados os valores representativos do grau de reputação de um peer. Entretanto, este método pode apresentar o problema do conluio. A utilização do segundo método reduz o número de buscas necessárias para o cálculo da reputação, permitindo uma maior escalabilidade e o desenvolvimento de aplicações mais eficientes, mas gera perda de precisão no cálculo da reputação, por usar somente uma fração das informações de reputação disponíveis na rede.

Com o objetivo de utilizar a reputação como forma de autenticar os usuários, o PGP [53] implementa um mecanismo conhecido como *Web of* Trust, no qual um usuário pode verificar a autenticidade da chave pública pertencente de outro usuário. Diferente do modelo centralizado de chaves pública, que utiliza uma Autoridade Certificadora (*Certificate Authority* – CA) para autenticação das chaves públicas, o modelo utilizado no *Web of Trust* utiliza um esquema distribuído aonde a autenticação de uma chave pública associada a um usuário é realizada por uma ou mais chaves públicas de outros usuários. Dessa forma, com o *Web of Trust* é possível somente validar se um usuário é autêntico ou não perante outros usuários, não sendo possível avaliar se o usuário é confiável para o uso de um recurso através da avaliação das ações realizadas pelo mesmo.

2.6.2 Trabalhos relacionados na área de Serviços Web

Mecanismos baseados em reputação vêm sendo utilizados como ferramentas eficientes para a descoberta e seleção de serviços [21], principalmente em ambientes onde não é desejado ou viável o estabelecimento de contratos eletrônicos tradicionais (SLAs). No âmbito acadêmico, sistemas de avaliação mais elaborados vêm sendo propostos. Os trabalhos apresentados em [34] e [35] descrevem modelos para seleção de serviços que levam em conta tanto parâmetros de QoS quanto a avaliação dos usuários. Os trabalhos [36, 37] propõem a utilização de avaliações de consumidores de serviços para determinar o valor monetário de transações eletrônicas. Nesses trabalhos, a reputação de um provedor é utilizada para ajustar o valor que um determinado provedor pode cobrar pelo fornecimento de serviços.

Nos trabalhos mencionados acima, a reputação é baseada na percepção que um consumidor tem com relação à utilização de um serviço, não sendo adequada para determinar o quão consistente é um serviço com relação a QoS realmente oferecida. Outro problema diz

respeito à confiabilidade da própria avaliação fornecida pelos clientes dos serviços [34, 38, 39]. Visando minimizar esses problemas, em [38] é proposto um modelo de cálculo de reputação que leva em consideração, além da avaliação dos clientes – denominada dimensão subjetiva de reputação – o histórico do valor de QoS efetivamente fornecido pelo provedor – denominada dimensão objetiva de reputação. Esse trabalho é estendido em [39], onde uma abordagem baseada em Lógica Nebulosa é utilizada para inferir o raciocínio associado a uma determinada avaliação subjetiva de um provedor. Esse raciocínio é então utilizado para detectar a formação de conluios, identificar preferências de usuários, e fornecer recomendações para os usuários. Esse trabalho é o que apresenta maior semelhança com o SATYA, sistema utilizado na presente proposta para o aumento da confiança do uso dos serviços fornecidos por provedores.

A diferença básica entre o SATYA e o trabalho de [39] é a forma de coleta dos valores de QoS efetivo e de utilização da avaliação subjetiva do usuário. Diferentemente de [39], a avaliação do usuário é utilizada não só para calcular valores de reputação de provedores, mas também para calibrar a freqüência de *probing* de uma entidade monitora de serviço. A vantagem dessa abordagem é o aumento de escalabilidade que advém da diminuição do número de mensagens necessárias ao funcionamento do sistema de reputação. Isso decorre do fato do SATYA receber valores de QoS efetivo somente quando é detectada uma discrepância entre os valores de QoS armazenados no monitor e os efetivamente percebidos pelo usuário. Um efeito secundário é a maior autonomia alcançada na arquitetura do SATYA. Como o SATYA não requer que a QoS efetiva seja constantemente informada pelo usuário, o acoplamento entre esses e o SATYA é mínimo, restringindo-se ao envio das mensagens de avaliação. Outra diferença importante em relação ao trabalho [39], é que o SATYA emprega uma arquitetura descentralizada, na qual uma rede P2P é sobreposta a rede que interliga os provedores e consumidores de Serviços Web. Os nós que compõem tal rede são responsáveis pelo armazenamento e gerenciamento dos valores de avaliações referentes aos provedores permitindo, desta forma, a descentralização do cálculo de reputação e conseqüente aumento de escalabilidade e robustez do sistema. Ainda, o SATYA tira proveito da comparação das avaliações subjetivas com as objetivas para o estabelecimento de grupos de preferência que são usados tanto como mecanismos de incentivo quanto como auxiliares no cálculo da reputação final de um provedor.

2.7 Considerações Finais do Capítulo

Neste capítulo, foram inicialmente apresentados os conceitos básicos necessários para o entendimento dos sistemas de reputação. Foram descritas as abordagens de arquitetura dos sistemas de reputação, seguido dos métodos para o cálculo da reputação e os principais problemas encontrados com o uso destes sistemas. Em seguida, foi abordado o tema das redes P2P que foram utilizadas no presente trabalho como infra-estrutura de comunicação entre os peers para a troca de informações sobre os valores de reputação. Também foi apresentado o conceito de Serviços Web. Foi também apresentada a Lógica Nebulosa, iniciando-se pelos conceitos básicos sobre conjuntos nebulosos e as formas de agregá-los e caracterizá-los através de índices escalares. Por último, foram expostos os trabalhos relacionados confrontando-os com a proposta deste trabalho. O próximo capítulo apresenta o sistema de reputação proposto, detalhando os métodos utilizados para o cálculo da reputação, o mecanismo de troca de mensagens de reputação e de combate para evitar o problema do conluio.

Capítulo 3 Sistema de Reputação Orientado a Serviços

Este capítulo apresenta um sistema de reputação orientado a serviços e baseado em lógica nebulosa, como forma de aumentar a confiabilidade dos serviços trocados entre estações. O sistema de reputação foi desenvolvido segundo uma estrutura modular, sendo que neste capítulo será apresentado o módulo denominado Módulo de Cálculo de Reputação, com o objetivo de realizar o cômputo da reputação em um cenário de uma Rede Metropolitana Sem Fio (RMSF) com topologia Malha (*Mesh*). No capítulo 4 o sistema de reputação proposto será estendido com a adição de novos módulos e utilizado em um cenário de ambiente de Serviços Web que utilizam uma Arquitetura Orientada a Serviços.

Em um cenário de uma RMSF com topologia Malha as estações podem interagir diretamente entre si, sem a intermediação de uma unidade central, dessa forma comportando-se como peers em uma rede P2P. Neste cenário, uma Estação-Assinante pode trocar informações com outras Estações-Assinantes, bem como, entrar e sair da rede, de forma autônoma. Para garantir que as estações possam trocar informações, um sistema de reputação pode auxiliar os usuários a localizar parceiros confiáveis e trocar serviços de maneira segura. Especificamente, este capítulo aborda o uso do sistema de reputação para o cálculo da reputação das estações clientes dos serviços fornecidos pelas estações provedoras.

Sendo assim, o Módulo de Cálculo de Reputação tem por objetivo o cálculo da reputação de um cliente de um determinado serviço. O módulo possui dois mecanismos: o Mecanismo de Busca de Reputação que tem o objetivo de obter os valores de avaliação sobre um peer cliente, e pelo Mecanismo de Cálculo da Reputação que realiza o cálculo da reputação. O Mecanismo de Busca de Reputação foi implementado utilizando uma rede Peer-to-Peer estruturada sobreposta a Rede Metropolitana Sem Fio, fornecendo as primitivas para a busca dos valores de reputação.

Além da infra-estrutura de trocas de mensagens, serão apresentadas as estruturas de dados utilizadas para armazenar as reputações dos peers, assim como, a forma de cálculo da reputação de um peer, através da utilização dos valores de reputação que este possui em um determinado serviço (reputação *peer-serviço*) utilizando Lógica Nebulosa.

Outro ponto que será apresentado são os mecanismos utilizados para a diminuição do impacto de avaliações maliciosas fornecidas por entidades em formação de conluio na reputação de um peer. Primeiramente é verificada a distribuição de freqüência das avaliações que um peer recebeu após o uso de diversos serviços, e em seguida, a aplicação de um filtro de forma a evitar oscilações (positivas ou negativas) na reputação deste.

Sendo assim, a Seção 3.1 apresenta uma descrição geral do sistema de reputação proposto, seguida da Seção 3.2 que mostra as estruturas de dados utilizadas pelo sistema de reputação. A Seção 3.3 apresenta o Mecanismo de Busca de Reputação baseado em uma rede Peer-to-Peer estruturada. A Seção 3.4 descreve o Mecanismo de Cálculo de Reputação, onde o sistema nebuloso de cálculo da reputação e os mecanismos para evitar o problema do conluio são detalhados. Por fim, a Seção 3.5 apresenta as conclusões do capítulo.

3.1 Descrição Geral

O Módulo de Cálculo de Reputação é composto por dois mecanismos: **Mecanismo de Busca de Reputação** e do **Mecanismo de Cálculo de Reputação**. O Mecanismo de Busca de Reputação é responsável pela busca dos valores de reputação dos nós distribuídos na rede, enquanto que o Mecanismo de Cálculo de Reputação é responsável por realizar o cálculo da reputação a partir dos valores retornados pelo Mecanismo de Busca de Reputação. A Figura 4 mostra os dois mecanismos presentes no Módulo de Cálculo de Reputação.

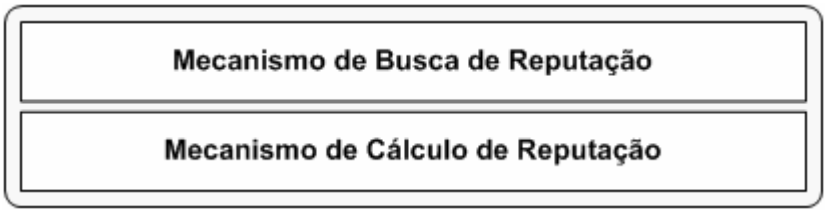


Figura 4 – Mecanismos do Módulo de Cálculo de Reputação

O **Mecanismo de Busca de Reputação** realiza uma busca pelos valores de reputação em uma rede Peer-to-Peer (P2P) implementada sobreposta a uma infra-estrutura de rede que pode ser representada por uma rede cabeada, uma rede sem fio local ou metropolitana, etc., conforme mostra a Figura 5. No plano inferior se encontra a infra-estrutura de rede onde estão mapeados todos os nós, enquanto que no plano superior está implementada a rede P2P. A rede P2P, por sua vez, é dividida em dois níveis: no nível inferior estão mapeados os nós da infra-estrutura de rede divididos em grupos denominados **Redes de Serviço** (RS), e no nível superior da rede P2P denominado de **Rede de Reputação** (RR) estão presentes alguns peers selecionados das Redes de Serviço que realizarão a tarefa de armazenar e calcular os valores de reputação de um peer cliente, assim como, intermediar a comunicação entre peers

pertencentes a diferentes Redes de Serviço. Os peers pertencentes a uma Rede de Serviço podem trocar serviços entre si ou entre Redes de Serviço diferentes, podendo um peer então atuar tanto como cliente ou provedor de algum serviço.

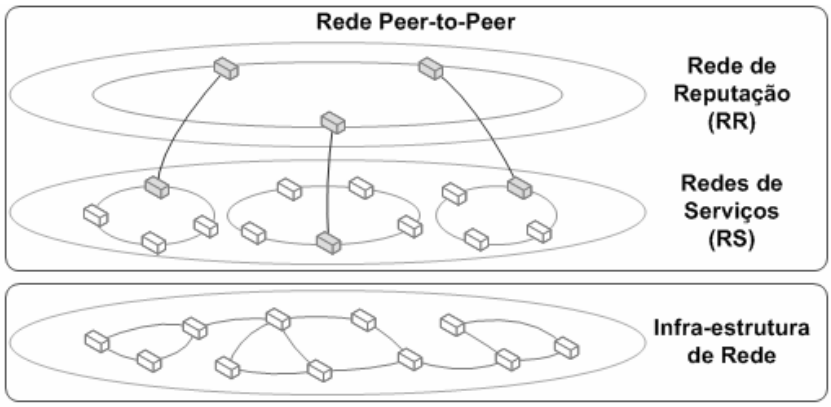


Figura 5 – Rede Peer-to-Peer implementada sobreposta a Rede Metropolitana Sem Fio

A rede P2P foi estruturada em dois níveis de forma a não impactar na escalabilidade da mesma e teve a sua topologia lógica baseada no trabalho [40]. De forma a contornar este problema, no trabalho [40] os nós de uma rede P2P são divididos em grupos (no presente trabalho denominados de Redes de Serviços), onde em cada grupo é implementado um protocolo que utiliza um algoritmo de *Tabela Hash Distribuída* (THD). Ao realizar esta divisão, o impacto da entrada e saída de peers somente afeta o grupo no qual o peer entrou ou saiu. A comunicação entre peers de diferentes grupos é realizada por peers especiais que atuam como roteadores das mensagens entre os grupos. Os peers que atuam como roteadores das mensagens são os peers que pertencem a Rede de Reputação e estes também estão conectados logicamente em um grupo. Uma característica desejável que estes peers devem possuir é de permanecerem longos períodos de tempo conectados a rede. Detalhes sobre a utilização desta arquitetura serão apresentados na Seção 3.3.

Após buscar os diversos valores de reputação que um peer possui, o **Mecanismo de Cálculo de Reputação** é utilizado para o cálculo da reputação do mesmo. Esse mecanismo usa Lógica Nebulosa para realizar o cálculo da reputação. A capacidade de manipular dados lingüisticamente imprecisos, através da manipulação de valores imprecisos ou subjetivos, como a determinação de um grau de reputação baixo, médio ou muito alto, faz com que a Lógica Nebulosa seja uma alternativa bastante adequada para a realização de cálculos de valores de reputação. Adicionalmente, uma vez que a Lógica Nebulosa é baseada em um conjunto de variáveis e regras do tipo *se-então*, o seu uso pode acarretar uma menor complexidade computacional, quando comparada com outros modelos, como as Redes Neurais, por exemplo.

O Mecanismo de Cálculo de Reputação utiliza basicamente como entrada para o cálculo da reputação dois valores: o valor de reputação do peer cliente e o de relacionamento que o peer que requisitou a reputação (isto é, o peer provedor) possui com o peer da rede P2P que forneceu. O valor de relacionamento representa o nível de confiança entre os dois peers (o peer que requisitou e o peer que forneceu a reputação). Peers fornecedores de reputação que possuem um baixo valor de relacionamento com o peer que requisitou a reputação terão pouca influência no cálculo de reputação, mesmo que estes forneçam altos valores de reputação.

O principal objetivo dos Sistemas de Reputação é permitir que seja inferido o comportamento futuro de um peer, baseado nas interações que este executou previamente com outros peers. Estes sistemas oferecem a possibilidade dos peers definirem políticas de acesso aos serviços e disponibilizarem serviços somente para peers que possuam um nível aceitável de reputação. Um exemplo de uma possível política de acesso seria a necessidade de um valor mínimo de reputação para o fornecimento ou não do serviço. Outro exemplo de política de acesso seria a verificação da presença do peer cliente do serviço em uma rede de relacionamento própria do peer provedor. Uma rede de relacionamento representa um conjunto de peers com o qual o peer provedor já interagiu previamente, isto é, são peers conhecidos e que possuem uma menor probabilidade de efetuar uma ação maliciosa.

As informações de reputação obtidas podem ser classificadas como privada ou global. Quando um peer provedor de serviço utiliza somente os valores de reputação de parte dos peers da rede P2P (isto é, de peers pertencentes à rede de relacionamento do peer provedor), os valores retornados representam um conhecimento privado que um peer provedor possui sobre um peer cliente. Informações privadas sobre um peer cliente são mais confiáveis, uma vez que se trata de uma informação obtida da rede de relacionamento envolvendo os peers cliente e provedor. Entretanto, tal informação pode ficar desatualizada devido à possibilidade de ambos os peers não trocarem serviços durante longos períodos de tempo.

Quando um peer provedor utiliza informações globais, isto é, informações fornecidas por todos os peers presentes ou não na sua rede de relacionamento, o valor de reputação pode representar um valor mais atualizado sobre o passado recente de uso dos serviços que o peer cliente utilizou. Entretanto, estas informações podem ser fornecidas por fontes pouco confiáveis, resultando em avaliações errôneas. Dessa forma, a conjugação destes dois tipos de informações (privada e global) pode resultar em uma informação mais atualizada (global) com as características de uma informação mais segura (privada).

Sendo assim, o Módulo de Cálculo de Reputação fornece dois valores de reputação de forma a avaliar o comportamento passado de um peer: a **Reputação Individual** e a **Reputação Agregada**. A Reputação Individual de um peer é obtida utilizando somente informações privadas de reputação, isto é, os valores de reputação retornados pelos peers da rede de relacionamento. Já a Reputação Agregada é obtida utilizando as informações globais que um peer possui, portanto, apresenta os problemas associados ao uso deste tipo de informação. De forma a desonerar a tarefa de cálculo da reputação de peers provedores ou clientes, os peers pertencentes a Rede de Reputação ficam responsáveis pelo cálculo de ambos os valores de reputação.

O valor da Reputação Individual é calculado em tempo real pelo peer da Rede de Reputação, isto é, no instante em que é necessária a descoberta da reputação de um peer cliente. Este valor de reputação apresenta um valor mais confiável, entretanto ela possui os problemas de apresentarem atrasos no seu cálculo e também na determinação da reputação de peers desconhecidos ou novos na rede.

De forma a contornar os problemas apresentados pela utilização da Reputação Individual, a Reputação Agregada é calculada pelo peer da Rede de Reputação utilizando todas as informações disponíveis a respeito de um peer. Após o fornecimento de um serviço, o peer provedor irá fornecer a avaliação de uso do serviço utilizado pelo peer cliente para o peer da Rede de Reputação atualizar o valor de Reputação Agregada e o armazenará em uma estrutura de dados que pode ser recuperada através de uma mensagem de solicitação de Reputação Agregada. Uma vez que este valor de reputação é calculado sempre após o fornecimento de um serviço, não existe o problema de quão atualizado é o valor da reputação referente aos serviços acessados pelo peer cliente. Entretanto, a Reputação Agregada apresenta o problema de ser mais vulnerável à ocorrência do problema de Conluio, de forma que são necessários mecanismos para minimizar este problema.

Toda vez que um peer provedor envia a avaliação de uso do serviço de um peer cliente para o peer da Rede de Reputação calcular e armazenar a Reputação Agregada, este utiliza dois mecanismos para minimizar o problema do Conluio. Primeiramente o peer da Rede de Reputação verifica a distribuição de freqüência de avaliações que o peer cliente recebeu, de forma a detectar avaliações fora do padrão de freqüência que este recebe. Após esta etapa, caso a avaliação esteja dentro do padrão de freqüência de avaliações recebidas pelo peer cliente, é aplicado um filtro que utiliza um sistema nebuloso para a atualização da Reputação Agregada. Para o cálculo da Reputação Agregada, assim como para o cálculo da Reputação

Individual, o sistema nebuloso leva em consideração tanto a reputação como o valor de relacionamento que o peer provedor possui com o peer cliente.

3.2 Funcionalidades do Módulo de Cálculo de Reputação

O Módulo de Cálculo de Reputação foi desenvolvido com a característica de calcular o valor de reputação baseado nas avaliações fornecidas pelos provedores de serviço e pelo uso do valor de relacionamento do provedor que forneceu a avaliação com o peer cliente. No presente trabalho, clientes e provedores de serviços utilizam um mecanismo de criptografia baseado em identidade [41, 42], de forma a identificarem cada peer e de assinar digitalmente as avaliações fornecidas.

No Módulo de Cálculo de Reputação proposto, o cálculo do valor da reputação é função do uso de um serviço por um peer, resultando em uma reputação associada ao par **peer-serviço**. As informações sobre os valores de reputação do par peer-serviço são armazenadas em duas tabelas: (i) **Tabela de Reputação Agregada** (TRA) que contém à reputação que um peer possui utilizando todas as informações disponíveis na rede a respeito deste peer, isto é, armazena a Reputação Agregada, e a (ii) **Tabela de Reputação Individual** (TRI), que contém os valores de avaliação que um peer provedor forneceu referente os serviços fornecidos para os diversos peers clientes pertencentes a rede de relacionamento do peer provedor. Os valores armazenados nesta tabela são utilizados para o cálculo da Reputação Individual de um peer cliente quando na requisição de um serviço. Ambas as tabelas ficam armazenadas nos peers da Rede de Reputação.

A Tabela de Reputação Agregada (TRA) possui um total de três campos: um campo que identifica à classe de serviço (IDS), um campo que identifica o peer (IDP), e o campo que representa o valor de Reputação Agregada que o peer possui (REP) na classe de serviço identificada no campo IDS. Já a Tabela de Reputação Individual (TRI) possui cinco campos: um campo para identificar à classe de serviço (IDS), um campo para identificar o peer (IDP), um campo para identificar o peer que informou a reputação (IDPI) do peer IDP, um campo AVA contendo o valor de avaliação do peer IDP na classe de serviço armazenada no campo IDS fornecida pelo peer que informou a avaliação (IDPI) e o campo REL representado o grau de relacionamento do peer IDP com o peer IDPI.

O campo IDS nas tabelas TRA e TRI tem como função identificar a classe de serviço no qual o valor de reputação/avaliação armazenado no campo REP/AVA está associado ao peer armazenado no campo IDP. Ou seja, um peer pode fazer uso de diversos serviços pertencentes a diferentes classes, e em cada classe possuir um valor de reputação/avaliação.

Uma vez que um peer possui um valor de reputação em uma classe de serviço, este pode utilizar este valor de reputação em outra classe de serviço, caso o peer provedor tenha como política de segurança a possibilidade de transferência da reputação da classe de origem do peer cliente. Outras políticas, como a utilização de valores médios de reputação do peer cliente pelas diversas classes de serviço existentes, ou de somente algumas classes consideradas mais importantes, também podem ser utilizadas pelo peer provedor.

Um peer, ao receber um valor de reputação/avaliação atribuído a um dado par peer-serviço para armazenar, utilizará os campos IDP e IDS em ambas as tabelas para identificar o peer e a classe de serviço associados ao valor de reputação/avaliação a ser armazenado.

O campo REP da Tabela de Reputação Agregada (TRA) armazena a Reputação Agregada do peer identificado no campo IDP e contém valores no intervalo [0, 1]. O campo AVA da tabela de Reputação Individual também contém valores no intervalo [0, 1], sendo que este campo armazena os valores de avaliação utilizados para o cálculo da Reputação Individual do peer identificado no campo IDP. O processo de busca e atualização do campo REP das tabelas TRA e TRI será explicado na Seção 3.3.

No campo REL da tabela TRI é armazenado o nível de relacionamento do peer armazenado no campo IDP com cada um dos peers armazenado no campo IDPI. Este campo é atualizado no decorrer das interações entre os diversos peers clientes do serviço (IDP) com cada um dos peers provedores (IDPI). A faixa de valores possíveis para este campo está no intervalo [0, 1], e quanto mais próximo de um, maior terá sido a quantidade de acessos do serviço e mais confiável será o valor da reputação armazenada no campo REP. O valor deste campo pode tanto ser incrementado quanto decrementado, dependendo das ações realizadas no acesso ao serviço. O valor de relacionamento será utilizado no cálculo da reputação das tabelas TRA e TRI de um peer, conforme será mostrado na Seção 3.4.

O cálculo do campo REL da tabela TRI é realizado da seguinte forma: para serviços acessados de forma correta pelo peer cliente, o campo REL é incrementado do valor 0,1 (crescimento linear). Quando um peer provedor ao fornecer um serviço detecta um comportamento anômalo no uso do serviço, o valor do campo REL é decrementado pela metade do valor atual (decremento exponencial). Esta forma de cálculo penaliza peers maliciosos quanto ao uso do serviço e será útil no cálculo da reputação utilizando a máquina de inferência nebulosa proposta no presente trabalho.

Outra estrutura utilizada é uma tabela denominada **Tabela de Relacionamento Local** (TRL) fornecida pelo peer provedor quando este envia uma requisição para o peer da Rede de

Reputação realizar o cálculo da reputação de um determinado peer cliente. Nesta tabela são armazenados os valores de relacionamento que o peer provedor possui para com diversos outros peers clientes com os quais já teve algum relacionamento (troca de serviços). O peer provedor irá fornecer estes valores armazenados localmente para o peer da Rede de Reputação calcular o valor de Reputação Individual do peer cliente, e a sua forma de atualização é a mesma do campo REL da tabela TRI. A sua utilização será descrita na Seção 3.3.

3.3 Descrição do Mecanismo de Busca de Reputação

Para implementar o Módulo de Cálculo de Reputação proposto é necessária a utilização de um mecanismo que facilite a busca, inserção e atualização dos dados referentes a reputação dos *peers*. Como premissa de utilização, este mecanismo não deve impactar na escalabilidade no cenário de aplicação utilizado. Para isso, o presente trabalho utiliza uma rede P2P estruturada organizada de forma hierárquica em dois níveis. No primeiro nível fica localizada a **Rede de Reputação** (RR) e no segundo nível as **Redes de Serviços** (RS). Em ambas as redes são utilizadas uma infra-estrutura P2P estruturada [43, 44, 45] que faz uso de um algoritmo de Tabela Hash Distribuída. Especificamente no presente trabalho foi escolhido a infra-estrutura que utiliza o Chord [43]. A RR é composta por peers que são responsáveis pelo armazenamento dos valores de reputação dos peers pertencentes a Rede de Serviço e também por intermediar a comunicação de diferentes Redes de Serviço. A Figura 6 mostra uma representação lógica da rede P2P, baseada no trabalho [40].

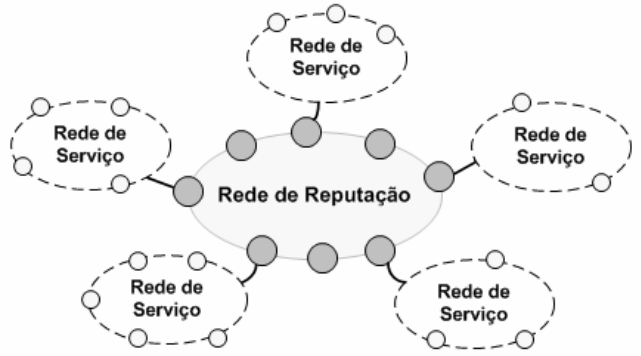


Figura 6 – Arquitetura Lógica da Rede de Reputação e das Redes de Serviço

Embora a utilização de um algoritmo de Tabela Hash Distribuída em uma rede P2P com um nível somente apresenta a vantagem de um menor consumo de mensagens (cerca de O (log n) mensagens para uma rede com n peers) para a recuperação de um valor de reputação na rede P2P, a atualização das estruturas de dados (tabelas de roteamento) para a manutenção da topologia em Anel torna-se bastante elevado em ambientes com um grande número de entradas e saídas dos peers. Além disso, caso os valores de reputação ficassem totalmente distribuídos pelos nós da rede P2P utilizando um algoritmo de THD, além do custo de

manutenção da topologia em Anel, com a atualização das tabelas de roteamento, haveria o custo de manutenção dos valores de reputação dos peers. Dessa maneira, a infra-estrutura de rede apresentada em [40] foi escolhida.

Sendo assim, baseada na rede P2P hierárquica, os peers pertencentes às Redes de Serviço podem atuar como clientes ou provedores de serviços. Caso um peer provedor de uma Rede de Serviço desejar obter o valor de reputação de um peer cliente, basta que o peer provedor envie uma mensagem de solicitação de cálculo da reputação do peer cliente para o peer da Rede de Reputação que faz a conexão da Rede de Serviço com a Rede de Reputação. Dessa maneira, o peer de uma Rede de Serviço fica responsável somente pelo provimento ou acesso a um serviço, desacoplando a tarefa do peer provedor de realizar o cálculo da reputação. A Figura 7 apresenta a seqüência de etapas para a obtenção do valor de reputação de um peer cliente.

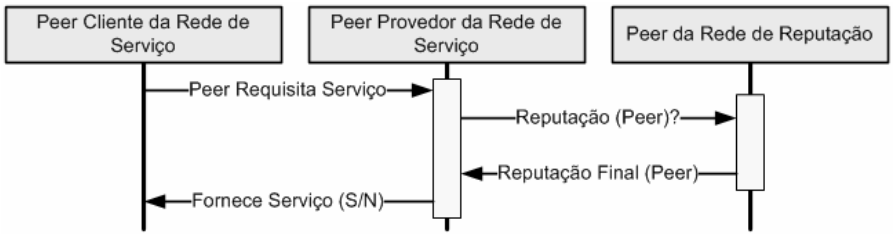


Figura 7 – Seqüência de etapas para a obtenção do valor de reputação de um peer cliente

Importante notar que não será necessariamente o peer que conecta a RS com a RR o responsável por realizar o cálculo da reputação. Ao receber a mensagem de solicitação de cálculo de reputação, o peer da RR irá utilizar as primitivas que o algoritmo de Tabela Hash Distribuída fornece para a descoberta do peer da RR responsável pelo armazenamento e cálculo da reputação do peer cliente. Após descobrir o peer da RR responsável pelo armazenamento e cálculo da reputação, a mensagem de solicitação de cálculo de reputação será encaminhada para este peer, que após realizar o cálculo da reputação, deverá enviar o valor de reputação para o peer da RR que conecta a RS na qual o peer provedor se encontra. Por fim, o peer da RR encaminhará o valor de reputação para o peer provedor.

Uma vez que os peers pertencentes à RR realizarão o armazenamento da reputação (isto é, armazenar a Tabela de Reputação Agregada (TRA) e a Tabela de Reputação Individual (TRI)) e o encaminhamento de mensagens entre as diversas RS, estes devem possuir a característica de permanecerem grandes períodos de tempo conectados a rede, de forma a não impactar na possibilidade de perda das reputações armazenadas pelas mesmas ao se desconectarem. Novas estações poderão ser adicionadas à rede RR de maneira dinâmica, de modo a não comprometer a escalabilidade da rede na qual o sistema esteja sendo utilizado.

Caso um peer da RR saia de operação durante um tempo indeterminado, um novo peer é escolhido da RS que foi desconectada da RR, de acordo com [40]. Durante este processo são atualizadas as tabelas de roteamento dentro da RS de forma a apontar para o novo peer que as conecta com a RR, assim como, as tabelas de roteamento dos peers conectados a RR para a manutenção da topologia em Anel. A inclusão do novo peer na RR provoca uma atualização na distribuição dos valores de reputação armazenados.

Os valores de reputação armazenados nos peers na RR possuem a característica de estarem redundantes em mais de um peer da RR, de forma que a saída de um peer desta rede não impacte na perda de informações a respeito da reputação. A redundância dos valores de reputação armazenados é obtida através da utilização de mais de uma função de *hash* para o armazenamento dos valores de reputação. Quando na ocorrência da saída de um peer da RR, os valores de reputação armazenados por este podem ser recuperados utilizando uma segunda função de *hash* utilizada previamente no armazenamento da reputação.

Uma estimativa do custo total de saltos de forma a um peer de uma RS acessar um serviço de um peer provedor em uma RS, utilizando um total de n peers e considerando que cada RS tenha um tamanho de log n peers e um total de n/log n peers na RR, em um caso estável (poucas saídas e entradas de peers) é de aproximadamente O(log (log n)) e em um caso instável (muitas entradas e saídas de peers) é de aproximadamente O(log n) [40]. Os custos ao utilizar uma rede DHT com um nível somente seriam de O(log n) no caso estável, e O(n) no caso instável [43]. A Tabela 1 apresenta um exemplo prático comparando o total de saltos para a obtenção de um recursos utilizando um DHT com um nível somente e um DHT Hierárquico, com um total (n=) 1000 peers, aonde 5% dos peers pertencem a RR e o tamanho de cada RS é de aproximadamente log n. No DHT Hierárquico é adicionado o valor 2, representando o roteamento entre a RS origem e destino, quando o caso.

Tabela 1 – Comparação do total de saltos utilizando um DHT com um nível somente e um DHT Hierárquico

	Estável	**Instável**
DHT com um nível	O(log n) = 10	O(n) = 1000
DHT Hierárquico Mesma Rede de Serviço	O(log(log n)) ≈ 1 + 2 = 3	O(log 1000) = 10 + 2 = 12

Quando os peers clientes e provedores de serviços pertencem a diferentes RS e os peers da RR encontram-se em um estado estável, o número de saltos é de aproximadamente O(log n/log n) + O (log (log n)) quando a RS está estável, e O(log n/log n) + O (log n) quando a RS está instável. Já para uma RR instável, o número de saltos é de aproximadamente

O(n/log n) + O (log (log n)) quando a RS está estável, e O(n/log n) + O (log n) quando a RS está instável. Os valores apresentados nesta Seção podem apresentar resultados diferentes, de acordo com o número de peers configurados para as redes RS e para a RR.

O benefício da utilização desta arquitetura de rede em detrimento de uma simples camada lógica sobreposta utilizando um protocolo DHT está no fato de (i) a utilização da RR, com a presença de peers que permanecem ativos durante longos tempos, contribui com uma diminuição no número de mensagens para a reorganização e estabilização da RR (isto é, das tabelas de roteamento de cada peer); (ii) como uma RS representa somente uma fração do tamanho total de uma rede, o processo de estabilização da RS após a entrada ou saída de um peer afeta somente a esta RS; (iii) ao criar uma estrutura hierárquica, o tamanho das tabelas de roteamento de cada peer diminui (dentro de cada RS de tamanho n, o tamanho das tabelas de roteamento é da ordem de O (log n), mais uma entrada apontando para o nó da RR). Em uma RR com n peers, o tamanho da tabela de roteamento é de O (log n).

3.3.1 Recuperação dos valores de reputação de um peer cliente

As etapas envolvidas na recuperação da reputação (Individual ou Agregada) de um peer na Rede de Reputação (RR) são semelhantes sobre a forma como é realizada. Primeiramente é aplicada uma função de *hash* no identificador do peer cliente que se deseja saber a reputação, obtendo o identificador do peer da RR responsável por armazenar a reputação. Para este peer da RR é enviada uma mensagem solicitando o valor de reputação (Agregada ou Individual).

A mensagem de requisição enviada para o peer da RR possui o seguinte conteúdo: o identificador do peer cliente, o identificador do peer provedor e uma *flag* que indica se a requisição é de um valor de Reputação Individual ou Reputação Agregada. Caso a flag esteja setada para a obtenção de um valor de Reputação Individual, também é enviada uma lista de valores de relacionamento contida na Tabela de Relacionamento Local (TLR).

3.3.1.1 Recuperação da Reputação Individual da Rede de Reputação

A Figura 8 mostra um exemplo onde um peer provedor A de um serviço deseja recuperar a reputação do peer cliente S. Nessa figura, a solicitação do peer S ao peer A é representada pela linha contínua. O peer S pode pertencer à mesma RS que o peer A ou não. Caso o peer S pertença a uma RS diferente da do peer A, a requisição será encaminhada pelos peers pertencentes a RR que conectam a RS do peer S com a RS do peer A

Ao receber a solicitação, o peer A executa duas funções de *hash* para a obtenção de duas identificadores distintos (representando os peers N e B) e, em seguida, envia uma

solicitação de reputação do peer S para um dos peers (por exemplo, peer N). Caso não receba resposta durante um certo tempo, o peer A envia a mesma solicitação para o peer retornado pela segunda função de *hash* (peer B). De forma a não comprometer a integridade das informações armazenadas nos peers da RR, todos os valores de reputação armazenados nesses peers são assinados digitalmente. Ou seja, quando um peer provedor envia um valor de reputação para um dos peers da RR armazenar, a reputação enviada por esse peer é assinada digitalmente utilizando a chave do mesmo. A linha tracejada da Figura 8 representa à interação de busca da reputação no peer N da RR.

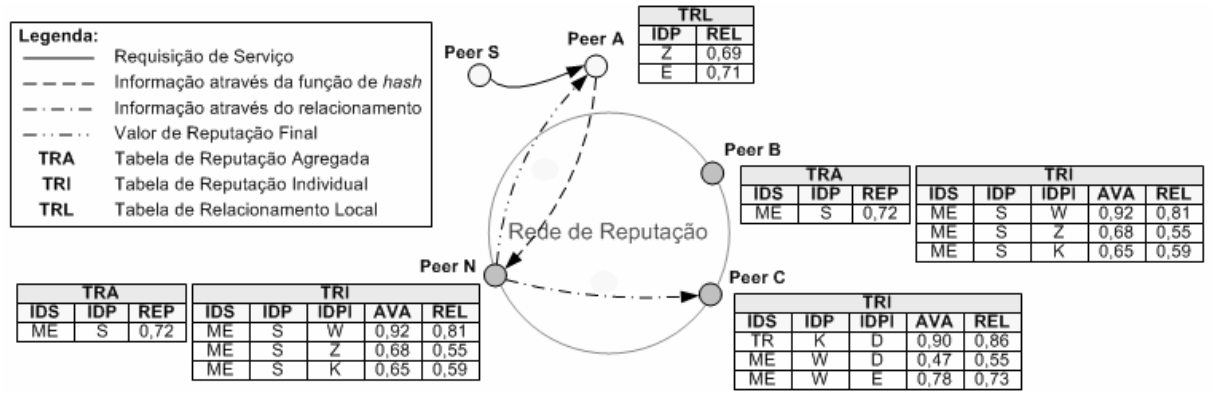


Figura 8 - Exemplo de busca de reputação utilizando o Mecanismo de Busca de Reputação

O peer N da RR armazena a reputação do peer cliente S, que utilizou os serviços dos peers W, Z e K, conforme mostra a TRI do peer N na Figura 8. Para o cálculo da reputação do peer S, o peer A envia na solicitação de cálculo de reputação para o peer N os valores de relacionamento presentes em sua Tabela de Relacionamento (os valores de relacionamento com os peers Z e E). O peer N necessita dos valores de relacionamento que o peer A possui com cada um dos peers da TRI (peers W, Z, K).

Entretanto, um peer provedor requisitante de um valor de reputação pode não possuir em sua Tabela de Relacionamento valores de relacionamento com todos os peers com os quais o peer cliente interagiu. Por exemplo, o peer A não possui nenhum valor de relacionamento com o peer S, possuindo somente o valor de relacionamento com o peer Z (0,69, da Tabela de Relacionamento do peer A). Para a obtenção dos valores de relacionamento com os peers W e K, o peer N da RR utilizará os valores de relacionamento fornecidos pelo peer A (com os peers Z e E) na descoberta dos valores de relacionamento com os peers W e K. A possibilidade de obtenção do valor de reputação a partir do relacionamento de um peer com terceiros é denominado de **Relacionamento Transitivo**.

O Relacionamento Transitivo representa o cálculo da reputação baseado no relacionamento com outros peers, informados na mensagem de solicitação da Reputação

Individual, que irá buscar na própria Rede de Reputação por valores de relacionamento com os peers desconhecidos para com o peer provedor, mais conhecidos pela sua rede de relacionamento.

Por exemplo, de posse dos valores de relacionamento fornecidos pelo peer A, o peer N utiliza uma função de *hash* para descobrir o peer da Rede de Reputação que armazena os valores de reputação dos peers W e K. O peer C é retornado como o responsável pelo armazenamento da reputação dos peers W e K. No peer C estão armazenados dois valores de reputação e relacionamento do peer W, respectivamente com os peers E e D. Uma vez que o peer D não foi informado pelo peer A como um peer presente em sua Tabela de Relacionamento Local, este valor é descartado, utilizando somente o valor de relacionamento do peer E. O relacionamento com o peer K da tabela TRI do peer C também é descartado, uma vez que no peer C não existe nenhum valor de relacionamento com os peers presentes na TRL do peer A (isto é, com os peers Z e E).

Sendo assim, uma vez que o peer provedor A não possui nenhum valor de relacionamento com o peer S, este utilizará os valores de relacionamento presente em sua TRL. Entretanto, este não utilizará diretamente os valores presentes na TRL como valores de relacionamento, e sim, será ponderado por estes valores. Por exemplo, o valor de relacionamento que o peer A possui com o peer S será o valor de relacionamento do peer A com o peer Z (0,69), ponderado pelo valor de relacionamento do peer Z com o peer S (0,55). O mesmo raciocínio é utilizado para obtenção do valor de relacionamento entre os peers A, E, W e S. A Tabela 2 resume os valores de relacionamento utilizados, assim como os valores de reputação, a partir do exemplo da Figura 8.

Tabela 2 – Valores Utilizados para o Cálculo da Reputação do Peer S

Peer	Reputação	Relacionamento
W	**0,92**	Rel_{A-E} (0,71) x Rel_{E-W} (0,73) x Rel_{W-S} (0,81) = **0,42**
Z	**0,68**	Rel_{A-Z} (0,69) x Rel_{Z-S} (0,55) = **0,38**

Uma estimativa do total de saltos para a mensagem de requisição de Reputação Individual de uma RS chegar até ao peer da RR responsável pelo armazenamento da reputação, considerando que a RR tem o tamanho de n/(log n) peers, é na ordem de O(log (n/log n)) saltos: um salto do peer da RS para com o peer da RR conectado e cerca de O(log (n/log n)) saltos até chegar ao peer da RR responsável por calcular a reputação. O peer da RR responsável por calcular a Reputação Individual poderá enviar mensagens para N peers da RR para a obtenção do valor de Relacionamento Transitivo, totalizando um total de N*O(log

(n/log n)) mensagens. Após obter os valores relacionamento o peer da RR responsável por calcular a reputação enviará o valor de Reputação Individual para o peer da RR que conecta a RS do peer provedor, mais um salto para deste peer da RR para o peer provedor. O total de mensagens geradas será de cerca de O(log (n/log n)) + N*O(log (n/log n)). Estes resultados são obtidos quando a RR apresenta-se estável. Para o caso em que a RR apresenta um comportamento instável, resulta em um total de O(n/log n) + N*O(n/log n) mensagens para a obtenção da Reputação Individual.

3.3.1.2 Recuperação da Reputação Agregada da Rede de Reputação

Caso um peer não possua nenhuma informação a respeito de um peer, isto é, ainda não tenha ocorrido nenhuma interação entre os dois, um possível valor de reputação que pode ser utilizado é o valor de Reputação Agregada. Este valor de reputação representa um valor global de reputação e é calculada toda vez que um novo valor de reputação é informado, a respeito de uma ação realizada pelo peer.

Conforme mostra a Figura 8, o peer provedor poderia utilizar somente o valor de Reputação Agregada que o peer S possui para permitir ou não o acesso ao serviço. Apesar de a Reputação Agregada representar um valor de reputação mais atual em relação aos serviços que o peer S utilizou, pode ocorrer o problema do conluio no cálculo deste valor de Reputação. Dessa maneira, fica a critério do peer provedor utilizar ou não o valor de Reputação Agregada.

O processo de recuperação do valor de Reputação Agregada de um peer é bastante simples: basta que o peer provedor envie uma mensagem de solicitação de Reputação Agregada para o peer da RR que conecta a RS do peer provedor com a RR. Ao receber esta solicitação, o peer da RR aplicará uma função de *hash* e identificará o peer da RR responsável por armazenar a Reputação Agregada do peer cliente. A mensagem de solicitação será então encaminhada para este peer que retornará o valor de Reputação Agregada, primeiro para o peer da RR que conecta a RS do peer provedor, que por fim, enviará a mensagem para o peer provedor. O resultado deste valor de reputação representa um passo mais rápido na sua obtenção, uma vez que o valor de reputação já está calculado. O processo de como será atualizado este valor de reputação será detalhado na Seção 3.4.2.

Seguindo o exemplo da Figura 8, o peer A envia uma mensagem para o peer N que conecta a RS do peer A com a RR. Uma vez que o próprio peer N é o responsável por armazenar o valor de Reputação Agregada do peer S (0,72), este retorna o valor de Reputação Agregada para o peer A. O custo total de saltos que a mensagem deve percorrer para obter o

valor de Reputação Agregada no caso que a RR apresenta-se estável e com tamanho de n/(log n) peers é na ordem de O(log (n/log n)) saltos: (i) Um salto do peer da RS para com o peer da RR conectado; (ii) O(log (n/log n)) dentro da RR para descoberta do peer que armazena a reputação; (iii) Um salto do peer da RR para o peer da RS. Já para o caso em que a RR apresenta-se instável, são necessárias cerca de O(n/log n) mensagens para a obtenção da Reputação Agregada.

3.3.2 Atualização do valor de Reputação Individual ou Agregada

O processo de armazenamento de um novo valor de reputação após a utilização de um serviço é efetuado da mesma forma como da obtenção do valor de reputação. Primeiramente, a mensagem contendo o novo valor de reputação é enviada para o peer da RR que conecta a RS do peer provedor que informa a avaliação do uso de um serviço por parte do peer cliente. Esta mensagem então é encaminhada para o peer da RR responsável por armazenar a reputação do peer cliente.

A mensagem de avaliação de uso de um serviço enviada pelo peer provedor possui o seguinte conteúdo: o identificador do peer cliente, o identificador do peer provedor, o valor de avaliação das ações executadas pelo peer cliente, e uma *flag* de relacionamento indicando que o serviço foi acessado de forma correta ou a indicação que o peer tentou efetuar uma ação maliciosa no acesso do serviço. O valor de reputação do campo AVA da TRI será atualizado para o novo valor de avaliação fornecida pelo peer provedor. Já o campo REP da tabela TRA será atualizado utilizando o processo descrito na Seção 3.4.2, aonde são utilizados os mecanismos para a minimização do problema do Conluio.

Já para a atualização do campo REL da TRI, caso a *flag* de relacionamento não esteja sinalizada, o peer da RR responsável por armazenar a reputação aumentará de 0,1 o valor armazenado no campo REL. Caso contrário, na ocorrência de uma ação maliciosa no uso do serviço e a sinalização da *flag*, o peer da RR diminuirá pela metade o valor armazenado no neste campo.

3.4 Descrição do Mecanismo de Cálculo de Reputação

Nesta Seção serão apresentados dois processos utilizados pelo peer da Rede de Reputação para o cálculo da Reputação Individual e Agregada de um par *peer-serviço* de um peer cliente. A diferença entre os dois processos é que para o cálculo da Reputação Individual são levados em consideração somente os valores de avaliação fornecidos pelos peers com o qual o peer provedor possui um valor de relacionamento, isto é, com o qual já interagiu. Para

o cálculo da Reputação Agregada são utilizados todos os valores de reputação disponíveis nos peers da Rede de Reputação.

Em ambos os processos são utilizados Sistemas Nebulosos para o cálculo da reputação. A Reputação Individual é resultado do uso dos valores de reputação e de relacionamento retornados pelo Mecanismo de Busca de Reputação e é acionado no momento em que um peer provedor envia uma solicitação a respeito da Reputação Individual de um peer cliente. A Reputação Agregada é executada toda vez que um peer provedor envia um novo valor de avaliação referente ao uso de um serviço por parte de um peer cliente.

3.4.1 Mecanismo de Cálculo da Reputação Individual

No processo de cálculo da Reputação Individual de um peer cliente, o peer provedor ao enviar os valores da Tabela de Relacionamento Local para o peer da RR calcular a reputação tem o objetivo de ponderar o valor de relacionamento que o peer provedor possui com os peers que já interagiram com o peer cliente. Os valores de relacionamento estão armazenados na Tabela de Reputação Individual (TRI) no peer da RR. Após a obtenção dos valores de avaliação e relacionamento através do Mecanismo de Busca de Reputação, a fórmula da Figura 9 é utilizada para o cálculo da Reputação Individual de um peer cliente.

$$\text{Reputação}_{\text{Provedor-Cliente}} = \frac{\sum_{\text{Peers}} \text{Cálculo de Reputação Individual } (\text{Avaliação}_{\text{Cliente}}, \text{Relacionamento}_{\text{Provedor-Peers}})}{\text{Total}_{\text{peers}}}$$

Figura 9 – Fórmula para o Cálculo da Reputação Individual de um peer cliente

Na fórmula da Figura 9, a Reputação Individual de um peer cliente para com um peer provedor é calculada através do valor médio da utilização do sistema nebuloso **Cálculo de Reputação Individual**. Para com cada peer da rede de relacionamento do peer provedor que fornece a reputação do peer cliente é calculado um valor de Reputação Individual utilizando como entradas a avaliação do peer cliente armazenada na tabela TRI e o relacionamento do peer provedor ponderado pelo valor de relacionamento com o peer que forneceu o valor de reputação do peer cliente.

O sistema nebuloso Cálculo de Reputação Individual foi implementado utilizando a ferramenta para a construção de Sistemas Nebulosos FIS Editor, presente no Matlab [46]. Para a sua construção devem ser criadas as bases semânticas, nas quais estão declaradas todas as variáveis lingüísticas do sistema nebuloso Cálculo de Reputação Individual.

Assim, esta etapa tem por objetivo definir os parâmetros da quádrupla das variáveis lingüísticas das bases de semânticas utilizadas no sistema nebuloso que constitui o Mecanismo de Cálculo de Reputação. O princípio adotado para o seu desenvolvimento foi de

aliar a confiabilidade do mecanismo em conjunto com a simplicidade no seu desenvolvimento. A confiabilidade do mecanismo de decisão está relacionada com a quantidade de conjuntos nebulosos (rótulos) definidos para cada uma das variáveis lingüísticas. Em relação à simplicidade, à medida que cresce o número de conjuntos nebulosos para aumentar a confiabilidade, os sistemas nebulosos que compõem o mecanismo tornam-se mais complexos de serem construídos e atualizados. Dessa maneira, foi estipulado um número de conjuntos nebulosos por variável lingüística de forma a não degradar excessivamente a confiabilidade inicial do mecanismo e, ao mesmo tempo, garantir a simplicidade dos sistemas nebulosos.

Foram criadas três variáveis lingüísticas para o sistema nebuloso Cálculo de Reputação Individual, sendo duas variáveis lingüísticas de entrada e uma de saída. As variáveis de entrada representam a reputação de um peer e o valor de relacionamento que o peer provedor possui com o peer cliente. A terceira variável lingüística representa o valor de reputação calculado. Na definição das duas primeiras variáveis lingüísticas, o primeiro elemento da quádrupla, nome da variável, foi declarado como sendo Grau-Reputação e Grau-Relacionamento para representar respectivamente os parâmetros reputação e relacionamento. O segundo elemento, referente aos rótulos dos conjuntos nebulosos, foi considerado para a variável Grau-Reputação os rótulos MB (Muito Baixo), BX (Baixo), ME (Médio), AL (Alto) e MA (Muito Alto) e para a variável Grau-Relacionamento os rótulos AM (Amigo), CO (Colega) e DS (Desconhecido).

Neste ponto cabe registrar que o número de rótulos para a variável lingüística Grau-Reputação foi baseada em Sistemas de Reputação similares [10, 11, 47, 48] que não utilizam Lógica Nebulosa. Nestes sistemas é utilizado um conjunto de cinco rótulos para o cálculo da reputação através das avaliações fornecidas pelos usuários e representa um valor suficiente para a sua utilização, sem aumentar a complexidade do sistema nebuloso. Para a variável Grau-Relacionamento foram utilizados três rótulos por representarem os mesmos conceitos de relacionamento utilizados pelos serem humanos.

O terceiro parâmetro, o universo de discurso, foi definido como o intervalo dos números reais [0, 1]. Quanto ao quarto elemento, a função de inclusão dos conjuntos nebulosos ou regras semânticas, foi considerada para ambas variáveis a função triangular. Para a variável Grau-Reputação, conforme pode ser visto na Figura 10, foram simulados cinco valores e criados cinco rótulos, onde foi utilizada a função triangular, uma vez que esta função relaciona um único elemento de um conjunto com um grau de inclusão com valor um (1).

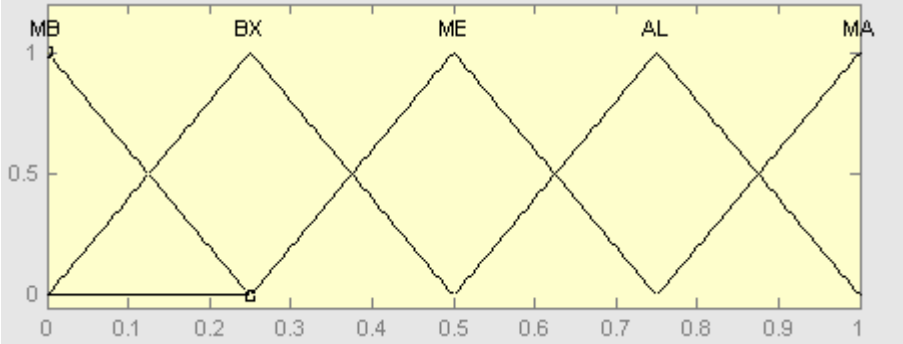


Figura 10 – Função de Inclusão – Variável Grau-Reputação

Já para a variável Grau-Relacionamento, foram simulados três valores e criados três rótulos, conforme mostra a Figura 11, utilizando uma função triangular.

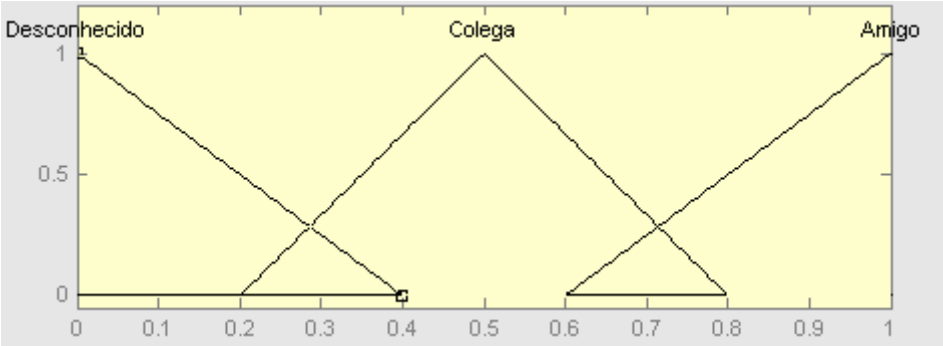


Figura 11 – Função de Inclusão – Variável Grau-Relacionamento

A última etapa é realizada pela máquina de regras difusas que determina quais regras serão ativadas pelos valores de entrada (variáveis lingüísticas Grau-Reputação e Grau-Relacionamento) a fim de determinar quais conjuntos nebulosos de saída sofrerão o processo de Desnebulização. A saída do Cálculo de Reputação Individual foi definida através da variável lingüística com nome Reputação, representando a reputação final calculada. Os rótulos considerados foram MB (Muito Baixo), BX (Baixo), ME (Médio), AL (Alto) e MA (Muito Alto). O universo de discurso está no intervalo [0,1] dos números reais e a função de inclusão utilizada foi a função triangular, conforme mostra a Figura 12.

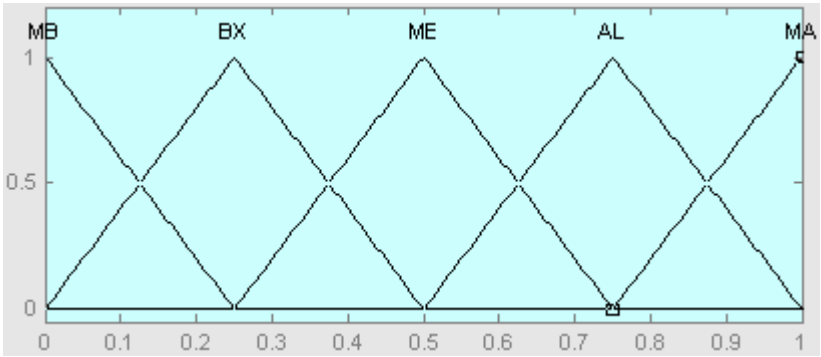


Figura 12 – Função de Inclusão – Variável Reputação

Com as variáveis lingüísticas definidas, o próximo passo é a definição das regras difusas. A definição das regras consiste em relacionar os conjuntos nebulosos das variáveis lingüísticas que participam do sistema por intermédio de expressões lógicas. Como a variável Grau-Reputação possui cinco conjuntos nebulosos distintos e a variável Grau-Relacionamento três, existem quinze possíveis formas de relacionar esses conjuntos nebulosos, onde cada relacionamento define um cenário de rede. Essas quinze regras difusas foram implementadas através do editor *Rule Editor* do *Fuzzy ToolBox* e estão descritas na Tabela 3.

Tabela 3 – Avaliador de Regras – Cálculo de Reputação Nebuloso

Regra	Regra Difusa
01	**If** (Grau-Reputação is MB) **and** (Grau-Relacionamento is DS) **then** (Reputação is MB)
02	**If** (Grau-Reputação is MB) **and** (Grau-Relacionamento is CO) **then** (Reputação is MB)
03	**If** (Grau-Reputação is MB) **and** (Grau-Relacionamento is AM) **then** (Reputação is MB)
04	**If** (Grau-Reputação is BX) **and** (Grau-Relacionamento is DS) **then** (Reputação is MB)
05	**If** (Grau-Reputação is BX) **and** (Grau-Relacionamento is CO) **then** (Reputação is MB)
06	**If** (Grau-Reputação is BX) **and** (Grau-Relacionamento is AM) **then** (Reputação is BX)
07	**If** (Grau-Reputação is ME) **and** (Grau-Relacionamento is DS) **then** (Reputação is MB)
08	**If** (Grau-Reputação is ME) **and** (Grau-Relacionamento is CO) **then** (Reputação is BX)
09	**If** (Grau-Reputação is ME) **and** (Grau-Relacionamento is AM) **then** (Reputação is ME)
10	**If** (Grau-Reputação is AL) **and** (Grau-Relacionamento is DS) **then** (Reputação is BX)
11	**If** (Grau-Reputação is AL) **and** (Grau-Relacionamento is CO) **then** (Reputação is ME)
12	**If** (Grau-Reputação is AL) **and** (Grau-Relacionamento is AM) **then** (Reputação is AL)
13	**If** (Grau-Reputação is MA) **and** (Grau-Relacionamento is DS) **then** (Reputação is ME)
14	**If** (Grau-Reputação is MA) **and** (Grau-Relacionamento is CO) **then** (Reputação is AL)
15	**If** (Grau-Reputação is MA) **and** (Grau-Relacionamento is AM) **then** (Reputação is MA)

Como um exemplo numérico do uso do Cálculo de Reputação Nebuloso, considere os valores apresentados na Tabela 2, obtidos pelo peer N da Rede de Reputação para calcular a reputação do peer S. Para calcular a reputação em relação ao peer Z são utilizados como entrada os valores de 0,68 para o valor de reputação e 0,38 para o valor de relacionamento. O processo de Cálculo de Reputação Individual retorna o valor de 0,414 como valor de reputação. A Figura 13 mostra a janela *Rule Viewer*, que compõe o programa *FIS Editor* e que permite a visualização gráfica do resultado da máquina de inferência Cálculo de Reputação Individual, a partir dos valores de entrada Grau-Reputação e Grau-Conhecimento e das regras ativadas.

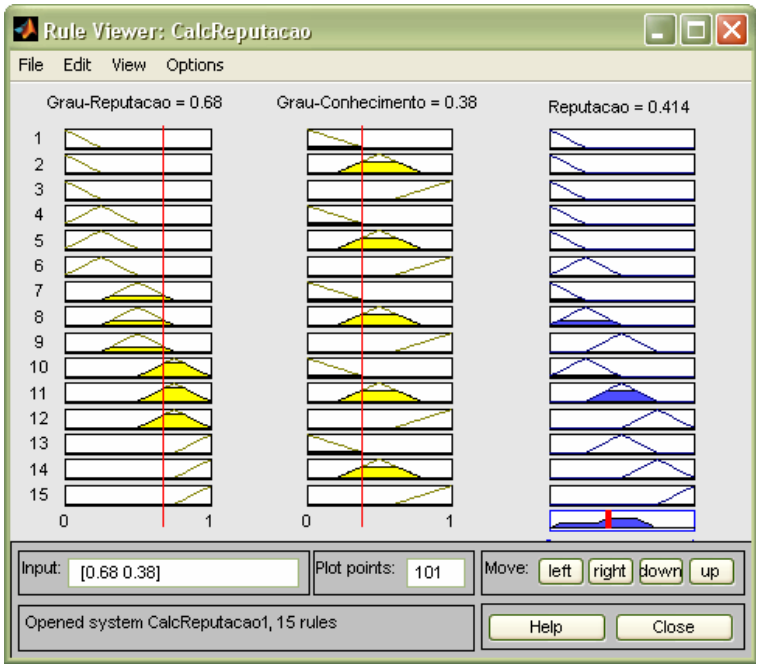


Figura 13 - Janela Rule Viewer do programa FIS Editor

Para calcular o valor de reputação utilizando o peer W, o valor de reputação utilizado será de 0,92 e o valor de relacionamento será de 0,42. O processo de Cálculo de Reputação Individual retorna o valor de 0,662 utilizando tais valores de reputação e de relacionamento.

De posse destes dois valores de Reputação Individual (0,414 e 0,662) é realizada uma média dos valores, retornando o valor de Reputação Individual de 0,54. Este valor é retornado para o peer A que pode fornecer ou não o serviço para o peer S, dependendo das políticas utilizadas por este para fornecer o serviço (por exemplo, para fornecer um serviço o peer deve possuir um valor de reputação mínimo de 0,50).

3.4.2 Mecanismo de Cálculo da Reputação Agregada

Uma vez que no cálculo da Reputação Agregada são utilizados todos os valores de reputação que os peers provedores fornecem, se faz necessária a utilização de mecanismos que minimizem a ocorrência do problema do conluio. Assim, toda vez que um peer da Rede de Reputação receber uma nova avaliação de um peer provedor, primeiramente esta avaliação será verificada quanto à natureza da distribuição de freqüência de valores de avaliação recebido pelo peer cliente e, em seguida, será aplicado um filtro para o cálculo e armazenamento final da reputação na tabela TRA.

3.4.2.1 Filtro na Distribuição de Freqüência dos valores de avaliação

O filtro de distribuição de freqüência funciona da seguinte forma: o peer da Rede de Reputação ao receber os diversos valores de avaliação para armazenar utilizará estes valores para montar uma tabela de freqüências de valores de avaliação. Após a formação da tabela,

resultado do recebimento de N valores de avaliação, são calculados a média e o desvio padrão dos valores de avaliação. O peer da Rede de Reputação ao receber um novo valor de avaliação, primeiramente será verificado se o novo valor pertence ao intervalo que compreende a X% dos valores de avaliação recebidos. Por exemplo, ao receber o valor 0,70 para armazenar, o peer da Rede de Reputação verificará se o valor 0,70 pertence ao intervalo que compreende a 95% dos valores recebidos até então pelo peer cliente. Caso este valor pertença ao intervalo, na segunda etapa de atualização da Tabela Grau de Reputação de Serviço é utilizado o filtro, mostrado na Seção 3.4.2.2.

Entretanto, o filtro pode não ser utilizado quando do recebimento de um baixo valor de reputação, indicando que pode ter acontecido um problema, como uma ação maliciosa do peer cliente no acesso ao serviço. Para evitar o uso da distribuição de freqüência, o peer da Rede de Reputação responsável pelo armazenamento da reputação verificará se o valor de relacionamento do peer provedor que informa o valor de avaliação do peer cliente que será armazenado possui o valor considerado muito alto (intervalo [0,8, 1,0]). Caso passe neste teste, o passo de uso da distribuição não é executado e é aplicado diretamente o filtro.

Esta etapa de não utilização da distribuição de freqüência é necessária para a diminuição imediata da reputação em caso de um evento, como um ataque ter sido detectado, e é utilizado somente em casos em que os dois peers possuem um alto valor de relacionamento.

3.4.2.2 Filtro para a Atualização da Tabela de Reputação Agregada

Após a etapa de verificação da utilização da distribuição de freqüências no novo valor de avaliação, tal valor não é imediatamente utilizado para a atualização do campo REP da Tabela de Reputação Agregada. Antes é executado um segundo processo com o intuito de evitar oscilações na atualização do grau de reputação e, conseqüentemente, diminuir a possibilidade de peers em processo de Conluio influenciarem o valor de reputação de um peer cliente. A fim de evitar oscilações abruptas na atualização dos graus de reputação de um peer cliente é utilizado o filtro da Figura 14.

$$Rep_{peer} = \alpha * Rep_{média} + (1-\alpha) * Ava_{nova}$$

Figura 14 – Fórmula para evitar oscilações na atualização da Reputação Agregada

Na fórmula da Figura 14 é atribuída a variável Rep_{peer} o resultado do cálculo da utilização dos valores de reputação média do peer cliente ($Rep_{média}$) e da nova avaliação (Ava_{nova}), baseado em um parâmetro α. Quanto maior for o valor de α, maior será o peso dado à reputação média do peer cliente. Ao invés de utilizar valores fixos de α para a utilização da

fórmula da Figura 14, neste trabalho está sendo utilizado um valor de α variável, dependente do valor de relacionamento e de reputação entre o peer provedor que está informando o valor de avaliação e o peer cliente que terá o seu valor de reputação alterado.

A utilização de um valor de α variável tem por objetivo diminuir que peers com pouco relacionamento ou com um baixo valor de reputação influenciem no valor de reputação do peer cliente em um dado par *peer-serviço*, evitando a criação de peers com o único objetivo de aumentar ou diminuir a reputação de um peer. Dessa maneira, quanto maior o grau de relacionamento, menor será o valor α (maior peso para Ava_{nova}), e vice-versa.

Dessa maneira, no processo de atualização do valor de Reputação Agregada de um peer cliente em um par *peer-serviço*, foi criada um sistema nebuloso aonde as variáveis lingüísticas utilizadas foram as mesmas no sistema Cálculo de Reputação Individual: Grau-Reputação e Grau-Relacionamento. A saída deste sistema nebuloso, o valor da variável α da Figura 14, foi definida através da variável lingüística com nome Alfa, com os seguintes rótulos: BX (Baixo), ME (Médio) e AL (Alto). O universo de discurso desta variável foi definido como sendo o intervalo [0,1] dos números reais e a função de inclusão utilizada foi a função triangular para o rótulo ME e para os rótulos BX e AL foi utilizado a função trapeizodal, conforme mostra a Figura 15. A Tabela 4 resume as regras utilizadas para a obtenção do valor final da variável Alfa.

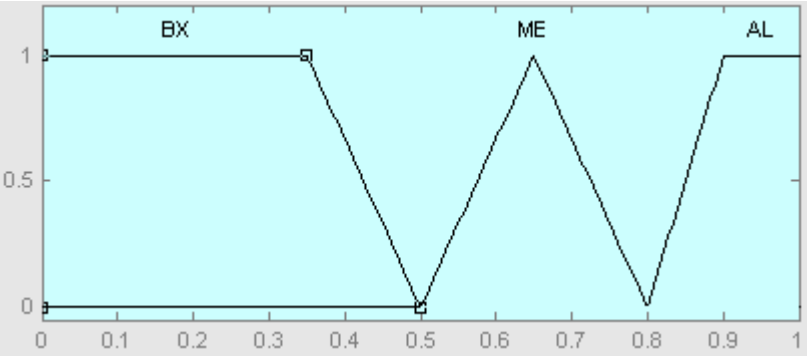


Figura 15 – Função de Inclusão – Variável Alfa

Tabela 4 – Avaliador de Regras – Atualização da Tabela de Reputação

Regra	Regra Difusa
01	**If** (Grau-Reputação is MB) **then** (Alfa is AL)
02	**If** (Grau-Reputação is BX) **then** (Alfa is AL)
03	**If** (Grau-Relacionamento is DS) **then** (Alfa is AL)
04	**If** (Grau-Reputação is ME) **and** (Grau-Relacionamento is CO) **then** (Alfa is ME)
05	**If** (Grau-Reputação is ME) **and** (Grau-Relacionamento is AM) **then** (Alfa is ME)
06	**If** (Grau-Reputação is AL) **and** (Grau-Relacionamento is CO) **then** (Alfa is ME)
07	**If** (Grau-Reputação is AL) **and** (Grau-Relacionamento is AM) **then** (Alfa is ME)
08	**If** (Grau-Reputação is MA) **and** (Grau-Relacionamento is CO) **then** (Alfa is BX)
09	**If** (Grau-Reputação is MA) **and** (Grau-Relacionamento is AM) **then** (Alfa is BX)

3.5 Considerações Finais do Capítulo

Neste Capítulo, foram apresentados os mecanismos propostos para diminuir o impacto da ação de peers maliciosos em processo de formação de conluio. O mecanismo de troca de mensagens utilizando um protocolo de Tabela Hash Distribuída permite que consultas a respeito da reputação de um peer sejam realizadas com um número bastante reduzido de mensagens.

Ao não acoplar a tarefa de cálculo de reputação de um peer cliente ao peer provedor do serviço diminui a sobrecarga no mesmo, e a utilização da divisão da rede em grupos torna o sistema escalável. Pode ocorrer dos peers que compõem a Rede de Reputação ficarem sobrecarregados, devido à quantidade de requisições de cálculo de reputação a ser realizado. Entretanto, novos peers podem ser adicionados a esta rede de forma dinâmica, de forma que tal aumento de sobrecarga pode ser rapidamente minimizado.

A utilização de um sistema que utiliza Lógica Nebulosa deveu-se a facilidade rapidez de aplicação do protótipo criado. Através da manipulação de regras de inferência e verificação dos resultados obtidos através da sua utilização, o sistema foi avaliado e adaptado para o cálculo da reputação. A utilização da utilização da distribuição de freqüência permite que avaliações feitas sem critério sejam descartadas e, em seguida, a utilização do filtro permite que o impacto de valores de avaliação fornecidos por peers desconhecidos seja mínimo no cálculo da reputação final.

Assim, é apresentada no Capítulo 4, a extensão do sistema de reputação em um cenários de Serviços Web que utilizam uma Arquitetura Orientada a Serviços, com o objetivo de aumentar a confiabilidade da utilização dos serviços fornecidos pelos provedores.

Capítulo 4 SATYA: Sistema de Avaliação de Provedores em um ambiente de Serviços Web

Este Capítulo apresenta o SATYA, uma extensão do Sistema de Reputação proposto no Capítulo 3 em um ambiente de Serviços Web que utiliza uma Arquitetura Orientada a Serviços. Nesse ambiente, o sistema proposto será adotado para fins de avaliação da reputação dos provedores de serviços. A sua adoção tem como objetivo prover um aumento da confiança no uso de transações de comércio eletrônico envolvendo a utilização de Serviços Web em ambientes abertos, isto é, ambientes em que o estabelecimento de contratos formais de Qualidade de Serviço (QoS) (através de uma SLA – *Service Level Agreement*) é indesejável ou apresenta um alto custo.

Em ambientes abertos onde provedores publicam valores de QoS para os serviços providos, torna-se necessária a adoção de mecanismos responsáveis por controlar e verificar se os valores publicados estão sendo corretamente fornecidos. A extensão do sistema de reputação proposto no Capítulo 3 utiliza os valores objetivos obtidos por entidades de monitoramento referentes ao fornecimento de um serviço por um provedor, em conjunto das avaliações subjetivas emitidas por clientes destes serviços, de forma a verificar a confiabilidade do provedor em respeitar as métricas de QoS publicadas.

Os valores objetivos e as avaliações subjetivas são comparados com o objetivo de: (i) validar as avaliações subjetivas; (ii) minimizar o nível de subjetividade dos valores de reputação calculados; e (iii) descobrir as preferências de provedores e clientes em relação às métricas de QoS. Ao atribuir ao provedor um valor de reputação, o SATYA incrementa a descrição do serviço publicado com o valor de reputação que pode ser utilizado durante a fase de descoberta do serviço pelos clientes. O valor de reputação representa o nível de confiabilidade de o provedor fornecer o serviço de acordo com as métricas de QoS publicadas.

Além disso, a comparação dos valores objetivos com as avaliações subjetivas permite que possam ser detectadas avaliações feitas sem critério ou que os valores objetivos estão desatualizados. Para tratar do segundo caso, o SATYA adota um mecanismo que ajusta dinamicamente a freqüência de *probing* de monitoramento, de forma a evitar um desperdício de envio de mensagens de monitoramento, entretanto, sem impactar no nível de atualização do valor armazenado.

Sendo assim, este Capítulo está organizado em cinco seções. Na Seção 4.1 é feita uma apresentação geral sobre o gerenciamento de QoS, dos mecanismos para monitoramento da QoS e do uso da reputação no aumento da confiança do uso de provedores que publicam as métricas de QoS. A Seção 4.2 apresenta a integração da extensão proposta em um cenário de Serviços Web que utiliza uma Arquitetura Orientada a Serviços. Em seguida, na Seção 4.3 é apresentada a inserção das entidades de monitoramento dos provedores na arquitetura de rede apresentada no Mecanismo de Busca de Reputação do Capítulo 3. A Seção 4.4 apresenta os módulos que compõem a extensão do sistema de reputação do Capítulo 3, e por fim, a Seção 4.5 finaliza o Capítulo com as considerações finais.

4.1 Gerenciamento da Qualidade de Serviço

Aplicações baseadas em Serviços Web são construídas a partir de contratos eletrônicos sintaticamente definidos utilizando-se a linguagem WSDL, ou seja, as operações, entradas e saídas esperadas e alguns detalhes de um determinado Serviço Web são descritos através de elementos WSDL. Contudo, para que seja possível estabelecer um contrato de prestação de serviços eletrônico entre um provedor de serviços e seu respectivo consumidor (ou cliente) é necessário que outros aspectos sejam tratados como, por exemplo, o estabelecimento de um conjunto de garantias de Qualidade de Serviço (QoS). Para tanto, a infra-estrutura de Serviços Web incorpora o conceito de SLAs (*Service Level Agrements*) [21, 19], que são acordos nos quais são estabelecidas as transações que necessitam ser realizadas, bem como a qualidade mínima exigida na execução destas. Desta forma, uma SLA auxilia na definição da divisão de responsabilidades entre os participantes de uma transação eletrônica.

Tradicionalmente, uma SLA é um acordo bilateral entre um cliente e seu respectivo provedor de serviço, o qual define um conjunto de parâmetros de QoS, tais como disponibilidade, vazão, tempo de resposta, etc., a ser garantido pelo provedor do serviço por ocasião da utilização do mesmo pelo cliente em questão. Entretanto, em ambientes com alto grau de dinamismo, o estabelecimento de um acordo formal e bilateral, como é o caso das SLAs tradicionais, pode não ser viável ou desejável. Um exemplo desse tipo de ambiente são os Serviços Web públicos do tipo *pay per use*, como os disponibilizados no site Amazon.com [20]. Como nesse tipo de serviço toda a Web pode ser vista como potencial cliente, o estabelecimento de SLAs tradicionais não é adequado devido, por exemplo, ao seu custo jurídico de estabelecimento. Nesse tipo de aplicação, o modelo bilateral dos SLAs pode ser substituído por um modelo aberto no qual o provedor do serviço publica os parâmetros de QoS do serviço em um registro [21]. Os potenciais consumidores do serviço podem então, se

basear na QoS publicada para selecionar os serviços de acordo com os requisitos de suas aplicações.

Para o funcionamento adequado dos contratos baseados em SLAs (tradicionais ou publicadas em um registro), tanto do ponto de vista do consumidor quanto do provedor do serviço, os parâmetros estabelecidos no uso de SLAs tradicionais ou no caso em que o provedor publica os parâmetros de Qos devem ser monitorados periodicamente de forma a verificar se a QoS real oferecida pelo serviço está compatível com a que foi a acordada ou publicada pelo provedor. No ambiente de Serviços Web que utiliza uma Arquitetura Orientada a Serviços, a função de monitoramento é normalmente realizada por terceiros, fato que advém da necessidade de não sobrecarregar o consumidor ou o provedor do serviço com a condução desta funcionalidade, e também da necessidade de garantia de resolução de conflitos no caso de uma das partes não confiar na outra.

Para fins de monitoramento dos níveis de QoS efetivamente entregues pelos provedores de serviços, entidades monitoras atuam como agentes responsáveis por verificar periodicamente a QoS provida por um provedor e por comparar com a QoS publicada ou acordada na SLA. Para tanto, os monitores devem armazenar valores de avaliação relativos a um provedor de serviço, denominados de **valores objetivos**, para os diferentes parâmetros de qualidade contemplados na SLA. A verificação dos parâmetros de QoS é usualmente feita através de mecanismos de *probing*, que consistem no estabelecimento de interações entre a entidade monitora e o provedor de serviço a ser monitorado. De forma a não sobrecarregar o ambiente, a freqüência dessa interação deve ser calibrada de modo a ser a mínima possível e, ao mesmo tempo, garantir a atualização da informação de QoS.

4.1.1 Problema na Freqüência de Atualização dos Valores Objetivos

Ao utilizar entidades monitoras para a avaliação da QoS provida por um provedor, pode ocorrer um problema de confiança relacionado à quão atualizada é a informação de QoS armazenada na entidade monitora em um determinado momento. O aumento na taxa de *probing* pode minimizar este problema, entretanto com o custo de aumentar a sobrecarga na rede e no processamento. Dessa forma, para a comunidade envolvida no desenvolvimento de aplicações de comércio eletrônico, torna-se crucial o fornecimento de mecanismos e de métodos para lidar com questões relacionadas à confiança em transações eletrônicas, sem impactar demasiadamente a tarefa de monitoramento.

De forma a aumentar a confiabilidade das métricas de QoS publicadas por um provedor, sem degradar os recursos de rede e processamento disponíveis, podem-se utilizar

avaliações subjetivas, que são informações fornecidas por clientes após a utilização de um serviço, em conjunto com os valores objetivos. Com a utilização destes dois valores (valores objetivos e avaliações subjetivas), pode-se gerar um valor mais atualizado referente às métricas de QoS do provedor, sem gerar um *overhead* demasiado alto de monitoramento.

O SATYA é um sistema que gerencia os valores de reputação de provedores de serviços, a partir de avaliações subjetivas fornecidas por clientes e de valores objetivos de QoS obtidos e armazenados pela entidade monitora. Este inclui mecanismos para calcular um valor de reputação de provedores, bem como para validar os valores de avaliações subjetivas fornecidas por clientes dos serviços. Quando ocorrem discrepâncias entre valores objetivos e avaliações subjetivas, tais ocorrências podem indicar que (i) ou o cliente que forneceu a avaliação subjetiva está se comportando de forma maliciosa (ii) ou o valor objetivo da entidade monitora pode estar desatualizado. Com o intuito de tratar a primeira opção, a utilização do histórico de valores objetivos e do último valor objetivo obtido para um provedor minimiza a ocorrência de avaliações subjetivas que tenham o intuito de causar danos a um provedor, diminuindo a reputação do mesmo.

Em relação à atualização dos valores objetivos obtidos por entidades monitoras, o presente trabalho propõe o uso de uma abordagem de ajuste dinâmico da freqüência de *probing*. A freqüência de *probing* é ajustada comparando os valores objetivos e as avaliações subjetivas fornecidas pelos clientes e por um valor de *threshold* que indica o quão atualizada estão os parâmetros de QoS armazenados. No momento da ocorrência de grandes discrepâncias na comparação dos valores objetivos e das avaliações subjetivas, assim como, o valor de *threshold* indicar que os parâmetros de QoS armazenados estão desatualizados, a freqüência de *probing* pode ser ajustada para um número maior de envio de mensagens de monitoramento, de forma a atualizar os parâmetros de QoS. Quando na não ocorrência de grandes discrepâncias entre os valores objetivos e avaliações subjetivas ou o valor armazenado não ultrapassar o *threshold*, a freqüência de *probing* pode ser diminuída novamente. A utilização desta abordagem, em detrimento de uma freqüência fixa de *probing*, permite uma maior escalabilidade e diminuição na carga de processamento e de rede do ambiente quanto ao número de mensagens de *probing* necessárias para a manutenção dos valores monitorados.

Outros problemas que podem ocorrer no momento em que são computadas grandes diferenças entre os valores objetivos e de avaliações subjetivas é a ocorrência de valores de QoS mal estipulados em uma SLA, formação de grupos de clientes maliciosos (processo de

Conluio), com o intuito de diminuir a reputação de um dado provedor, e também, o fornecimento de uma avaliação imprecisa fornecida por um cliente. Estes problemas podem ser minimizados através da utilização dos valores históricos de fornecimento de um serviço, de forma a permitir o ajuste dinâmico dos valores acordados, diminuir o impacto da formação de clientes em um processo de Conluio, ou minimizar a ocorrência de uma avaliação incorreta.

4.1.2 Uso da Reputação no Processo de Descoberta de Serviços Web

Em um ambiente de Serviços Web, o processo de descoberta de serviços é realizado através da utilização de entidades conhecidas como registros, aonde são armazenadas informações relacionadas às interfaces de acesso disponibilizadas em um documento WSDL. Dentro da arquitetura de Serviços Web, uma entidade denominada de UDDI pode ser utilizada nesta tarefa. Entretanto, registros UDDI não fornecem mecanismos de descoberta e seleção de serviços baseados em suas capacidades e comportamento em relação a um determinado conjunto de métricas de QoS.

A possível adição de metadados referentes às métricas de QoS de um determinado serviço permitirá que um cliente possa realizar a descoberta e consulta de um serviço de provedores mais capacitados. Entretanto, a somente divulgação das métricas de QoS não é suficiente, uma vez que ocorre a necessidade de mecanismos para garantir que a QoS publicada no registro é efetivamente fornecida pelos provedores.

No processo de avaliação provido pelo SATYA, o valor de reputação gerado, referente ao serviço fornecido por um provedor, pode também ser disponibilizado no registro UDDI, de forma que um cliente possa consultá-lo no momento de descoberta do serviço. Este valor de reputação refletirá a reputação do provedor em fornecer o serviço nas métricas de QoS publicadas por este. Para o cômputo da reputação, o SATYA utiliza os valores objetivos e as avaliações subjetivas fornecidas, e através da utilização de um sistema nebuloso é computado o valor de reputação, que pode então ser utilizado pelos clientes em conjunto com outros descritores do serviço buscado.

4.1.3 Seleção de Provedores de Serviços em função dos Grupos de Preferência

A partir dos valores objetivos de cada métrica de QoS obtidos pelas entidades monitoras, o SATYA realiza um **cálculo de conformidade** em cada métrica, que indica o quanto o provedor tem cumprido o valor da métrica de QoS publicada. De posse dos valores de conformidade, o SATYA cria **grupos de preferência**, os quais consistem em grupos de provedores que possuem características similares de fornecimento de serviço em relação a

uma determinada métrica de QoS. Também são criados grupos de preferência de clientes, sendo que para estes são utilizadas as avaliações subjetivas fornecidas para a determinação do grupo de um cliente.

Com respeito aos grupos de preferência de clientes, um grupo pode conter clientes que possuem a tendência de preferir uma determinada métrica de QoS em detrimento de outras (por exemplo, clientes que preferem provedores que fornecem um serviço com o menor tempo de resposta possível, podem formar um grupo de preferência). Para ilustrar a criação de grupos de preferência de clientes, o SATYA pode, ao analisar o resultado de um serviço oferecido por um provedor e uma avaliação subjetiva fornecida por um cliente, detectar a métrica principal em que o cliente se baseou para fornecer a sua avaliação. Baseado nesta análise, o cliente pode ser inserido em um grupo de preferência de uma determinada métrica. O mesmo acontece com a criação de grupos de preferência de provedores, sendo que os valores utilizados são os valores objetivos obtidos pelas entidades monitoras.

O resultado da criação de grupos de preferência de servidores e clientes no sistema proposto tem como objetivos: (i) atuar como um mecanismo de incentivo, para estimular clientes a fornecerem avaliações, e (ii) auxiliar o processo de seleção de provedores, restringindo a escolha dos clientes a provedores de seu próprio grupo de preferência. Ao fornecerem avaliações subjetivas, clientes podem ser beneficiados com a possibilidade de selecionar provedores que possuem uma característica desejada pelos mesmos, uma vez que, provedores de um determinado grupo de preferência possuem a tendência a fornecer um “melhor serviço” no grupo em questão.

4.1.4 Avaliação da Reputação de um Provedor

Baseado no valor de avaliação subjetiva fornecida por um cliente em conjunto com o valor de relacionamento entre o cliente e o provedor avaliado, o Módulo de Cálculo de Reputação apresentado no Capítulo 3 é utilizado para calcular um valor de reputação para o provedor em questão. Entretanto, este valor subjetivo pode ter sido fornecido baseado em uma tendência individual de métrica de QoS, isto é, a avaliação pode ter sido influenciada por uma métrica de preferência utilizada por um cliente. Por exemplo, no caso em que um cliente possui uma tendência a avaliar melhor provedores que fornecem serviços na métrica tempo de resposta, provavelmente este cliente fornecerá avaliações ruins para provedores que fornecem um “melhor serviço” em outra métrica que não a métrica tempo de resposta.

De forma a contornar este problema e utilizando os grupos de preferência de Provedores e de Clientes, um cliente poderá requisitar para o peer da Rede de Reputação o

cálculo da reputação de um provedor utilizando somente os valores de reputação de clientes que pertençam ao seu grupo de preferência. Por exemplo, utilizando o cálculo de Reputação Individual apresentada no Capítulo 3, um cliente que possui a tendência a preferir provedores que provêem um melhor serviço na métrica tempo de resposta enviará requisições para obter os valores de reputação do provedor somente para clientes que possuem a tendência nesta métrica, isto é, para os clientes que pertencem ao grupo de preferência tempo de reposta.

Ao não utilizar os valores da Rede de Relacionamento apresentada no Capítulo 3 para o cálculo da Reputação Individual, pode ocorrer o problema do conluio, uma vez que podem ser recebidas avaliações fornecidas por peers com o qual nunca interagiu. Entretanto, este problema é minimizado devido ao descarte de avaliações feitas sem critério quando na comparação realizada entre os valores objetivos obtidos pela entidade de monitoramento e das avaliações subjetivas.

4.2 Integração do SATYA em um Ambiente de Serviços Web

O SATYA foi concebido para ser incorporado a sistemas que utilizam Serviços Web baseados em uma Arquitetura Orientada a Serviços, conforme mostra a Figura 16. Na Figura 16, o provedor publica além de um documento WSDL, as métricas de QoS que o provedor se dispõe a respeitar. O SATYA utiliza as métricas de QoS publicadas e os valores objetivos obtidos pela entidade de monitoramento denominado **Monitor de Desempenho** [19] de forma a verificar se o provedor está respeitando as métricas de QoS publicadas. Os clientes ao realizarem uma busca pelo serviço no Agente de Serviços, poderão informar as métricas de QoS desejadas, assim como, a reputação mínima do provedor. O SATYA realiza então o cálculo da reputação utilizando as avaliações subjetivas e incrementa a descrição do provedor no Registro com a reputação calculada.

Em um ambiente aberto como a Web, a publicação das métricas de QoS pode ser realizada por provedores confiáveis ou não, tornando-se necessária a utilização de mecanismos para avaliar se a QoS publicada pelo provedor é a realmente oferecida. O SATYA fornece o mecanismo de avaliação da QoS publicada, incluindo o valor de reputação do provedor referente as métricas de QoS publicadas.

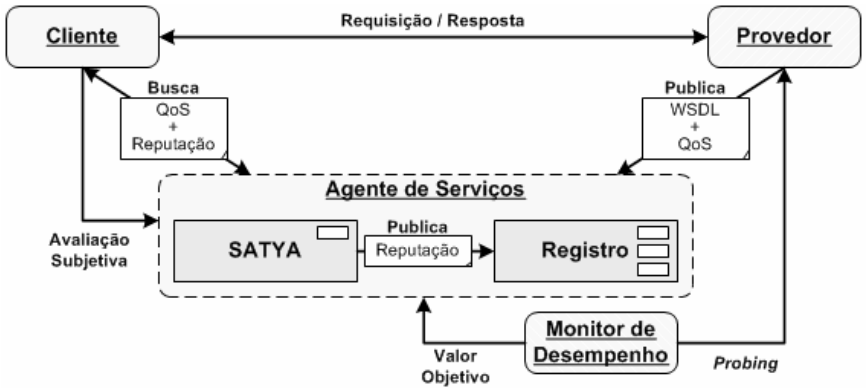


Figura 16 – SATYA integrado a um ambiente de Serviços Web

A interação entre consumidores e provedores de serviço é monitorada pelo Monitor de Desempenho, responsável pela recuperação dos valores objetivos obtidos por *probing*. A atividade de *probing* possibilita a coleta dos valores de QoS efetivamente fornecidos pelo provedor do serviço. Ao mesmo tempo, os clientes, após a utilização de um serviço, enviam as suas avaliações subjetivas para o agente de serviços. De posse dos valores objetivos e das avaliações subjetivas, o SATYA (i) recebe e valida as avaliações de utilização de serviços enviadas pelos consumidores de serviços (avaliações subjetivas); (ii) realiza o cálculo de conformidade e tendência; (iii) estabelece grupos de preferência de provedores e clientes; (iv) gerencia os valores de reputação dos provedores; e (v) armazena os valores referentes às avaliações e preferências de consumidores/provedores.

Assim, no SATYA são levadas em conta tanto as avaliações subjetivas fornecidas por clientes que utilizaram previamente os serviços quanto às avaliações objetivas obtidas pelo Monitor de Desempenho. A validação dos valores de avaliação fornecida por um cliente é feita através da comparação destes com os valores objetivos gerados. Tal comparação serve para evitar a formação de grupos de clientes maliciosos, que comprometam o uso de um serviço, ou mesmo para evitar avaliações levianas, feitas sem critério. Além disso, esta comparação também serve para ajustar a freqüência de *probing* adotada pelo Monitor de Desempenho.

Quanto aos grupos de preferência, o seu objetivo é o de separar clientes/provedores em grupos segundo critérios de similaridade. Com relação aos clientes, os grupos referem-se a sua preferência de avaliação dos serviços quanto aos parâmetros de QoS. Com relação aos provedores, o grupo de preferência diz respeito às métricas de QoS que os mesmos tendem a fornecer com valores mais altos. A criação dos grupos de preferência de provedores baseia-se na premissa de que, uma vez que um provedor forneça um “melhor serviço” em uma

determinada métrica, ele terá grandes chances de continuar a fornecer o “melhor serviço” naquela mesma métrica, em requisições futuras.

Os grupos permitem, então, que clientes dêem preferência para acessar provedores que pertençam ao seu próprio grupo, isto é, provedores que ao longo de sua utilização não desrespeitaram a métrica de QoS publicada do grupo em questão. Adicionalmente, clientes podem usar a informação de grupos de preferências de outros clientes para orientar seu processo de seleção de serviços, da mesma forma que ocorre com Sistemas de Recomendação [49, 50]. Ao buscar os valores de reputação de um provedor antes de utilizar seus serviços, o cliente dá um peso diferente à reputação reportada por clientes que possuem preferências similares a dele. O fato de o cliente ter acesso a avaliações de clientes com preferências similares as suas também funciona como um mecanismo de incentivo, estimulando o cliente a fornecer avaliações, já que ele irá se beneficiar das avaliações dadas por outros.

Quanto à geração de valores de reputação, o mecanismo possui o objetivo de aumentar a confiança nas transações eletrônicas, no que se refere à qualidade do serviço oferecido, fornecendo para os clientes destes serviços uma medida representativa de sua confiabilidade.

4.3 Infra-estrutura de Monitoramento

Devida à importância do Monitor de Desempenho no SATYA e dos Agentes de Serviço, e visando obter uma arquitetura escalável e robusta, a alocação lógica dos peers responsáveis pela atividade de monitoramento e agente é feita utilizando-se a Rede de Reputação (RR) apresentada no Capítulo 3. Os peers pertencentes à RR, e, portanto, escolhidos para desempenharem o papel de monitoramento, podem ser peers especificamente designados para esse papel ou os próprios peers que atuam como clientes e/ou provedores de serviços. A Figura 17 apresenta uma possível configuração lógica dos peers na Rede de Reputação.

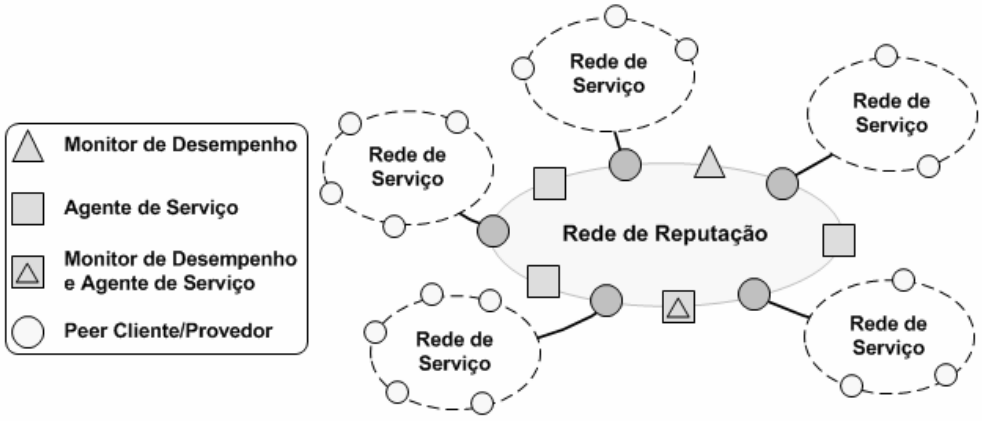


Figura 17 – Peers Monitores de Desempenho na Rede de Reputação

A partir da Figura 17, os clientes podem selecionar provedores através do envio de mensagens de consulta aos Agentes de Serviço contendo, além das descrições funcionais dos serviços desejados, as métricas de QoS requeridas. O custo total de mensagens enviadas pelos clientes é a mesma apresentada na Seção 3.3 do Capítulo 3 para a consulta da Reputação Agregada de um peer cliente.

Para a realização do monitoramento, o peer que atua como Monitor de Desempenho envia mensagens em intervalos de tempo definidos através da comparação das avaliações fornecidas por clientes e pelos próprios valores obtidos nas mensagens de monitoramento, e de um valor de *threshold* que indica o quão atualizado está o valor monitorado. Quando é detectada alguma grande discrepância entre estes dois valores (avaliação e os valores de monitoramento), ou ultrapassar o valor do *threshold*, o peer Monitor de Desempenho diminui o intervalo de tempo de envio de mensagens, aumentando a sobrecarga na rede. Por outro lado, quando os valores comparados apresentam pequenas diferenças, tal intervalo de envio de mensagens pode ser aumentado.

4.4 Descrição dos Módulos do SATYA

O SATYA é composto por cinco módulos: Módulo de Cálculo de Conformidade (MCC), Módulo de Cálculo de Tendência (MCT), Módulo de Determinação de Preferência de Provedores (MDP), Módulo de Determinação de Preferência de Clientes (MDC), e Módulo de Cálculo de Reputação, o qual foi apresentado no Capítulo 3. A Figura 18 mostra uma composição genérica dos módulos e a sua seqüência de ativação, sendo que o Módulo de Cálculo de Reputação é ativado independente dos outros módulos.

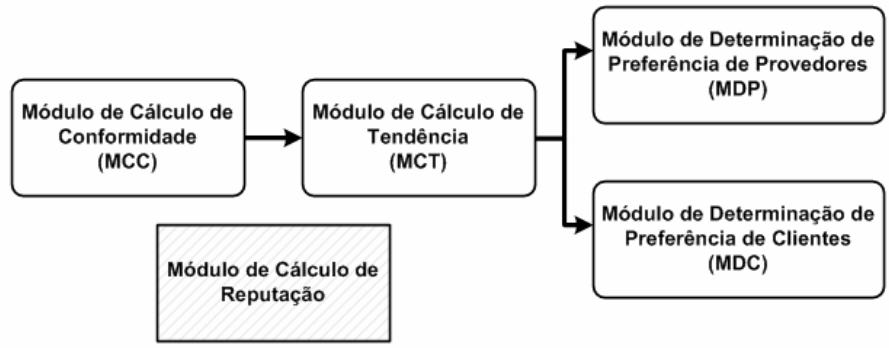


Figura 18 – Módulos do SATYA

O MCC possui a função de verificar o nível de conformidade que um provedor possui com o serviço fornecido a respeito das métricas de QoS publicadas. O resultado deste módulo serve como entrada para o MCT, que retorna os valores de tendência em cada métrica de QoS publicada. O MCC computa internamente dois valores de conformidade em relação às métricas de QoS publicadas: um valor de conformidade que leva em consideração um

conjunto de dados históricos de fornecimento de serviço e um valor de conformidade que utiliza o último valor de utilização do serviço. O primeiro valor de conformidade será utilizado para o cálculo de tendência de provedores, enquanto que o último será utilizado para o cálculo de tendência de clientes.

O MDP difere do MDC com relação ao algoritmo utilizado para a criação dos grupos de preferência de provedores e clientes, e quanto ao número de entradas. O MDP utiliza como entrada somente os valores de tendência retornados pelo MCT em cada métrica de QoS, utilizando os dados históricos de fornecimento do serviço. Já o MDC utiliza os valores de tendência retornados pelo MCT calculados utilizando o último valor de fornecimento do serviço, mais a avaliação subjetiva fornecida pelo cliente.

O uso dos valores históricos e do último valor de fornecimento do serviço são utilizados para o cálculo de conformidade de provedores e clientes, respectivamente. A utilização destes valores para o cálculo de tendência e dos grupos de preferência para provedores e clientes é devido ao fato que provedores possuem uma menor probabilidade de mudança de tendência ou de grupo de preferência que clientes. Um provedor de serviço possui uma tendência a fornecer um “melhor serviço” em uma determinada métrica devido a alguma característica intrínseca do mesmo, como um enlace de maior banda ou um grande poder de processamento. Já clientes utilizam informações pessoais no fornecimento de avaliações, e com isso, tendem a mudar de tendência sobre a melhor métrica de QoS em determinados espaços de tempo durante a utilização dos diversos serviços.

Por fim, utilizando as avaliações subjetivas e o nível de relacionamento que o cliente possui com os provedores, o cálculo da reputação é realizado pelo Módulo de Cálculo de Reputação, já apresentado no Capítulo 3.

A seguir são descritos os quatro novos módulos apresentados, com respeito as suas entradas, saídas, funcionalidades e objetivos de uso.

4.4.1 Módulo de Cálculo de Conformidade (MCC)

O MCC é utilizado para calcular o valor de conformidade para um dado provedor de serviço, o qual é baseado nos valores das métricas publicadas e nos valores das mesmas métricas obtidas pelo Monitor de Desempenho. Para cada métrica de QoS utilizada no sistema há um valor de conformidade associado. Diferentemente do trabalho apresentado em [39], este módulo foi desenvolvido com o intuito de levar em consideração o histórico de serviços oferecidos por um provedor para o cálculo da conformidade.

Uma questão importante para a realização do cálculo de conformidade é a validação dos valores obtidos para as métricas quando da utilização do serviço. No SATYA os dados de QoS efetivamente fornecidos são obtidos através de *probings* realizados pelo Monitor de Desempenho.

Idealmente, os parâmetros reportados em cada métrica avaliada não devem apresentar diferenças entre os valores publicados e os obtidos quando do uso do serviço. Entretanto, nem sempre isso ocorre. Por um lado, o envio de *probes* com uma freqüência muito grande por parte das entidades de monitoramento pode não ser escalável e, ao mesmo tempo, resultar em um aumento da carga do provedor, afetando seu desempenho (ou seja, o processo da medição estaria influenciando os resultados da própria medição). Por outro lado, o envio de *probes* com uma freqüência muito pequena pode produzir avaliações desatualizadas no monitor. Para obter freqüências de *probing* que reflitam o estado atual dos provedores e ao mesmo tempo não gerem sobrecarga, a estratégia adotada pelo SATYA é realizar a comparação sistemática entre os valores objetivos e as avaliações subjetivas de avaliação dos serviços. Ou seja, comparar os valores objetivos provenientes de medidas, com os subjetivos, fornecidos por clientes, para validar ambos, um contra o outro. Essa comparação é realizada como parte das funcionalidades do módulo MDC (Seção 4.4.3).

O mecanismo proposto pelo MCC é uma extensão do método apresentado em [39]. Em [39] é utilizado um método denominado **Cálculo de Conformidade**, que tem como entradas os valores das métricas de QoS que foram publicadas e os valores das métricas correspondentes resultantes do uso do serviço e, como resultado final, o valor de conformidade do serviço, conforme mostra a Figura 19.

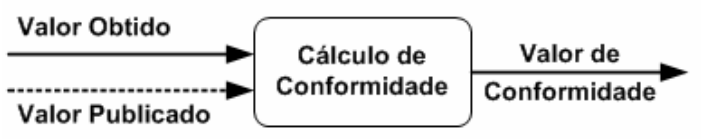


Figura 19 – Cálculo de Conformidade

Seja $A_{publicado}$, o valor da métrica de QoS A publicada pelo provedor e A_{obtido}, o valor final da métrica de QoS A referente ao fornecimento do serviço. O Valor de Conformidade da métrica de QoS A na j-ésima vez será dado pela fórmula da Figura 20.

$$\text{Valor de Conformidade}_j = (A_{publicado,j} - A_{obtido,j})/A_{publicado,j}$$

Figura 20 – Fórmula do Cálculo de Conformidade

A fórmula da Figura 20 mostra que o valor de conformidade apresenta-se no intervalo $]-\infty, 1[$. No caso do MCC, a faixa de valores foi truncada no seu limite inferior em -1. Dessa

maneira, o valor de conformidade situa-se no intervalo [-1, 1[. Esta expressão também mostra que valores negativos ou positivos de conformidade significam que a QoS efetivamente provida está abaixo ou acima dos valores publicados, respectivamente. No caso de um valor de conformidade assumir o valor zero (Valor de Conformidade$_j$ = 0), os valores publicados e os obtidos são iguais.

Para ilustrar o funcionamento do MCC, suponha que um provedor publica a métrica Tempo de Resposta do serviço (TR) de 250ms e o valor obtido da correspondente métrica ao ser efetivamente utilizado o serviço foi de 200ms. Usando a fórmula para o Cálculo de Conformidade, obtém-se como resultado o valor 0,2 de conformidade, indicando que o peer cumpriu o estabelecido no SLA e forneceu o serviço abaixo do valor acordado. O resultado da avaliação subjetiva fornecida pelo cliente deste serviço será provavelmente alta, caso o cliente não esteja em processo de Conluio.

Entretanto, caso o provedor publique para a mesma métrica o valor de 100ms e o valor obtido ao ser usado o serviço for da mesma forma 200ms, o resultado de conformidade será de -1,0, indicando que o provedor não cumpriu o estabelecido no SLA, fornecendo o serviço bem abaixo da métrica estabelecida. De acordo com os exemplos mencionados anteriormente, o provedor de um serviço deve estabelecer acordos SLA para as métricas de forma que o valor objetivo final na métrica em questão não tenha como resultado um valor muito baixo (próximos de -1). Entretanto, muitas vezes os valores de QoS publicados não refletem de forma realista os valores entregues na maior parte dos casos. Portanto, ajustes dinâmicos, que reflitam de modo mais realista o que ocorre na prática, são uma forma de tornar os valores publicados mais confiáveis.

A extensão do MCC apresenta a contribuição de realizar o cálculo da conformidade de provedores levando em consideração à média dos últimos valores obtidos do uso do serviço. O valor de conformidade que leva em consideração somente o último valor obtido no uso do serviço será utilizado para calcular o grupo de preferência do cliente. Já o valor médio dos últimos valores obtidos será utilizado para: (i) evitar que oscilações no oferecimento de um serviço por parte de um provedor influenciem a sua reputação; (ii) minimizar a possibilidade de um provedor manipular os valores acordados de QoS de forma a aumentar a sua reputação; e (iii) determinar o grupo de preferência do provedor. A Figura 21 mostra o uso do MCC para o cálculo de conformidade de provedores e clientes.

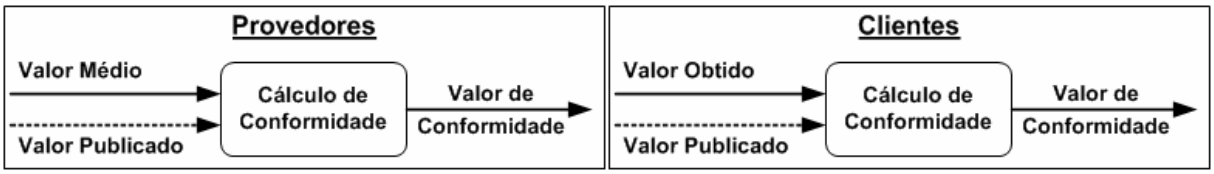


Figura 21 - Valores de entrada do MCC para provedores e clientes

Como um exemplo do uso do valor de conformidade, suponha que a métrica TR publicada seja de no máximo 800ms. Considere o valor de TR obtido para uma utilização do serviço como sendo 200 ms e a média dos oito últimos valores obtidos a partir de utilizações prévias deste serviço como sendo 220 ms. Para tais valores, o valor de conformidade utilizando o último valor obtido é de 0,75 e o valor de conformidade utilizando a média dos oito últimos valores obtidos é de 0,725. Como o valor de conformidade utilizando os dados históricos de fornecimento do serviço é alta, próximo de 1, isto indica que para a métrica TR publicada não reflete o estado atual em relação aos últimos valores providos. Dessa maneira, isto pode indicar que o valor publicado da métrica TR não está atualizada. Por outro lado, se o valor de conformidade histórico fosse próximo de zero, isto indica que o valor publicado está atualizado.

Um outro exemplo com os mesmo parâmetros utilizados no exemplo anterior, mas utilizando um valor médio dos oito últimos valores obtidos de 750ms, o valor de conformidade é de 0,062, indicando que o valor acordado está conforme o seu valor histórico de fornecimento de serviço e, portanto, atualizado. O valor de conformidade do último valor obtido (200 ms) indica que o provedor forneceu o serviço com um tempo bem abaixo do seu valor histórico, resultado de uma possível baixa utilização do mesmo.

O cálculo do valor de conformidade baseado nos valores médios de fornecimento do serviço pode ser utilizado para amortizar os impactos referentes a anomalias no fornecimento de QoS como, por exemplo, os casos onde um provedor esteja passando por um momento de sobrecarga atípica. Esse tipo de situação é facilmente identificável analisando o valor de conformidade histórica e o uso do SATYA permite excluir os valores de avaliação obtidos nessas situações.

De acordo com os exemplos mencionados anteriormente, um peer provedor de serviço deve publicar valores de QoS e/ou estabelecer SLAs com valores bem próximos a sua média histórica de fornecimento do serviço, uma vez que, caso o mesmo realize acordos com valores bem inferiores ou superiores a sua média de fornecimento, o cálculo de conformidade retornará um valor próximo de 1 ou -1, respectivamente, o que influenciará no cálculo final de sua reputação.

Cabe lembrar que, para um dado serviço, o valor de conformidade refere-se a uma métrica específica, portanto um provedor de serviços possui vários valores de conformidade, um para cada métrica avaliada.

4.4.2 Módulo de Cálculo de Tendências (MCT)

O MCT tem como função calcular uma série de valores de avaliação do uso do serviço baseados em uma possível tendência ou preferência por uma métrica específica de QoS, a partir dos resultados fornecidos pelo MCC. Além disso, o MCT também realiza um cálculo de avaliação de uso de um serviço sem tendência por uma métrica específica. Dessa maneira, a partir dos valores de tendência calculados pelo MCT e em conjunto com a avaliação subjetiva fornecida pelos clientes, o SATYA poderá determinar a preferência de clientes e provedores por uma métrica de QoS, através dos módulos de determinação de clientes e provedores descritos na Seção 4.4.3.

Os valores de conformidade em cada métrica de QoS retornados pelo MCC servem de entrada para o MCT, sendo que o valor de conformidade calculado utilizando os valores históricos serve de entrada para o cálculo de tendência de provedores, e o último valor de fornecimento para o cálculo de tendência de clientes. A **Figura 22** mostra o funcionamento geral do módulo MCT.

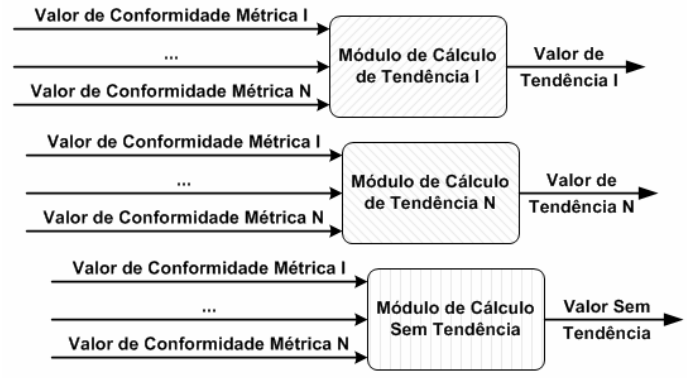


Figura 22 - Módulo de Cálculo de Tendências

O MCT apresenta-se como uma extensão do sistema nebuloso apresentado em [39], que tem como objetivo simular o processo de inferência do raciocínio humano ao fornecer uma avaliação subjetiva. Nesta extensão, para o cálculo dos valores de tendência foram adicionadas novas variáveis nebulosas e definidos diferentes conjuntos de regras de inferência. O primeiro conjunto trata todas as métricas como iguais, isto é, calcula um valor de avaliação sem tendências em relação a uma métrica específica de QoS. Os demais conjuntos de regras de inferência, cada um, levam em consideração uma métrica como sendo mais importante que as outras. Dessa maneira, para um total de N entradas de valores de

conformidade, são calculados N valores de tendência, mais um valor sem tendência. A Figura 23 mostra a implementação do sistema nebuloso no presente trabalho, aonde foram levadas em consideração três métricas de QoS: Tempo de Resposta (Conformidade-TR), Disponibilidade (Conformidade-DS) e Desempenho (Conformidade-DE). Como resultado, são retornados três valores de tendência (Tendência-TR, Tendência-DS e Tendência-DE), uma para cada métrica, e um valor sem tendência (Sem-Tendência).

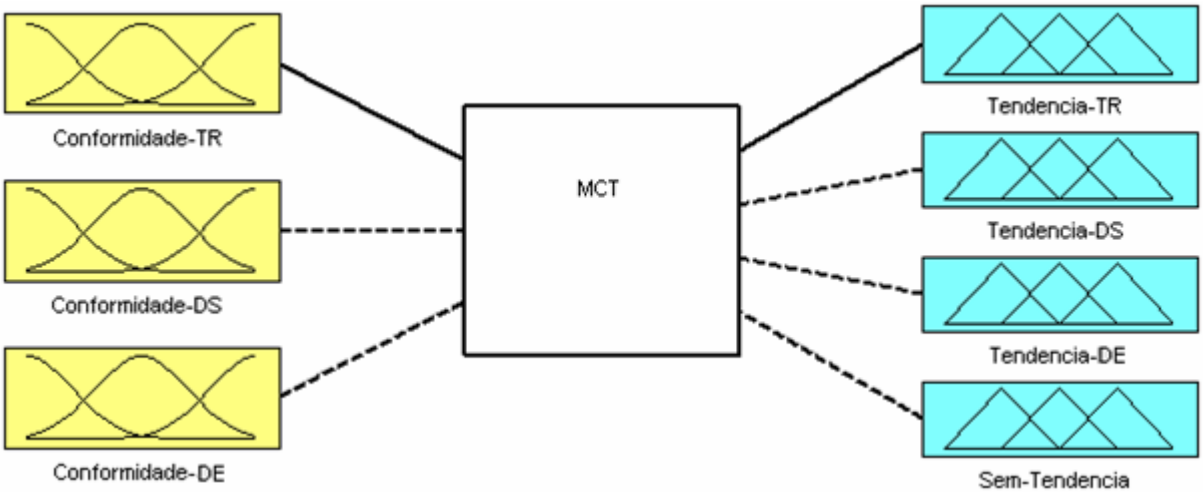


Figura 23 – MCT implementado com as métricas Tempo de Resposta, Disponibilidade e Desempenho.

No sistema nebuloso apresentado, as variáveis Conformidade-TR, Conformidade-DS e Conformidade-DE possuem os seguintes rótulos: CMB (Conformidade Muito Baixa), CBX (Conformidade Baixa), CON (Conforme), CAL (Conformidade Alta) e CMA (Conformidade Muito Alta). Foram utilizados cinco rótulos para essa variável ao invés de três utilizadas no trabalho [39]. O universo de discurso de cada variável está no intervalo dos números reais [-1, 1[. A função de inclusão dos conjuntos nebulosos ou regras semânticas considerada foi a função triangular, conforme mostra a Figura 24.

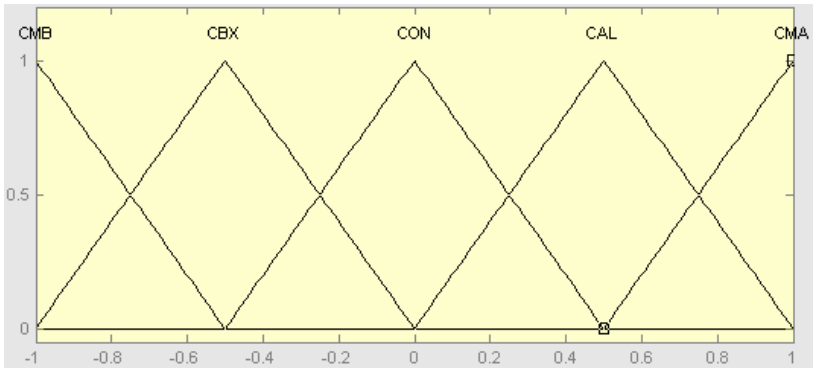


Figura 24 – Função de Inclusão das variáveis Conformidade-TR, Conformidade-DS e Conformidade-DE

A máquina de regras difusas determina quais regras serão ativadas pelas entradas fornecidas (variáveis lingüísticas Conformidade-TR, Conformidade-DS e Conformidade-DE)

a fim de determinar quais conjuntos nebulosos de saída sofrerão o processo de Desnebulização. As saídas do sistema nebuloso do MCT foram definidas através das variáveis lingüísticas Tendência-TR, Tendência-DS e Tendência-DE para o cálculo de tendência nas métricas tempo de resposta, disponibilidade e desempenho, mais a variável Sem-Tendência aonde é retornado um cálculo sem tendência. Os rótulos considerados para cada uma das variáveis de saída foram TMB (Tendência Muito Baixa), TBX (Tendência Baixa), TME (Tendência Média), TAL (Tendência Alta) e TMA (Tendência Muito Alta). O universo de discurso foi definido no intervalo [0,1] dos números reais e a função de inclusão utilizada foi a função triangular, conforme mostra a Figura 25.

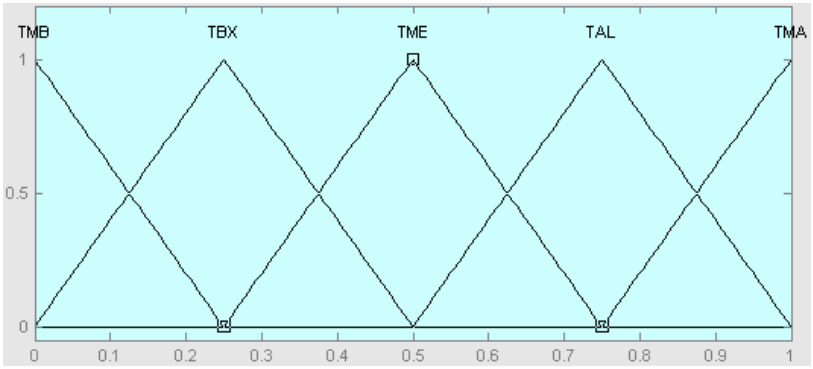


Figura 25 - Função de Inclusão das variáveis Tendência-TR, Tendência-DS e Tendência-DE e Sem-Tendência

Por fim, a Tabela 3 mostra as regras difusas que o módulo MCT utiliza para o cálculo dos valores com tendência em cada métrica de QoS. O Apêndice A apresenta o conjunto de regras utilizado para o cálculo sem tendência. No presente trabalhos foram levados em consideração somente a tendência em uma determinada métrica ou em nenhuma métrica. Um possível trabalho futuro poderia ser a criação de regras difusas que levam em tendência duas ou mais métricas de QoS (por exemplo, tempo de resposta e disponibilidade) em detrimento de outras.

Tabela 5 – Avaliador de Regras com tendência a uma determinada métrica de QoS

Regra	Regra Difusa
01	**If** (Conformidade-TR is CMB) **then** (Tendência-TR is TMB)
02	**If** (Conformidade-TR is CBX) **then** (Tendência-TR is TBX)
03	**If** (Conformidade-TR is CON) **then** (Tendência-TR is TME)
04	**If** (Conformidade-TR is CAL) **then** (Tendência-TR is TAL)
05	**If** (Conformidade-TR is CMA) **then** (Tendência-TR is TMA)
06	**If** (Conformidade-DS is CMB) **then** (Tendência-DS is TMB)
07	**If** (Conformidade-DS is CBX) **then** (Tendência-DS is TBX)
08	**If** (Conformidade-DS is CON) **then** (Tendência-DS is TME)
09	**If** (Conformidade-DS is CAL) **then** (Tendência-DS is TAL)

10	**If** (Conformidade-DS is CMA) **then** (Tendência-DS is TMA)
11	**If** (Conformidade-DE is CMB) **then** (Tendência-DE is TMB)
12	**If** (Conformidade-DE is CBX) **then** (Tendência-DE is TBX)
13	**If** (Conformidade-DE is CON) **then** (Tendência-DE is TME)
14	**If** (Conformidade-DE is CAL) **then** (Tendência-DE is TAL)
15	**If** (Conformidade-DE is CMA) **then** (Tendência-DE is TMA)

4.4.3 Módulos de Determinação de Preferência de Provedores (MDP) e de Determinação de Preferência de Clientes (MDC)

Para a criação e atualização de grupos de preferência de provedores, o MDP utiliza um sistema de pontuação simples, que tem como entrada os valores de tendência retornados pelo MCT. Os valores retornados pelo MCT são armazenados em uma tabela denominada **Tabela de Preferências de Provedores** (TPP). Toda vez que as métricas de QoS providas no uso de um serviço forem informadas (valores objetivos), o valor atual do campo referente a essa métrica será incrementado do novo valor. Dessa maneira, para a descoberta da preferência de um provedor, basta verificar em todos os campos de preferência da Tabela de Preferências de Provedor, aquele campo que possui o maior valor associado a uma determinada métrica. De tempos em tempos é aplicado um processo que normaliza os valores da tabela TPP de forma a evitar que cresçam indefinidamente.

Já o MDC tem por objetivo avaliar a opinião fornecida pelo cliente quanto ao serviço provido (valor subjetivo) em função dos valores de tendência retornados pelo MCT e, assim, criar grupos de preferência de clientes segundo uma determinada métrica. O objetivo da criação de grupos de preferência é permitir que clientes de um determinado grupo de preferência utilizem serviços nos quais poderão obter uma melhor qualidade de serviço, assim como possibilitar a formação de redes sociais [51], que são comprovadamente uma forma de aumentar a confiança nas transações eletrônicas.

Como entradas, o MDC recebe os valores de avaliação de tendência, retornados pelo MCT, e o valor subjetivo informado pelo cliente do serviço, para um dado serviço utilizado. O valor subjetivo consiste em um único número, que traz implícito o raciocínio por trás da avaliação dada pelo cliente, ou seja, a métrica que o mesmo julga mais relevante ao avaliar um serviço. Um dos objetivos do módulo proposto é justamente tornar explícito esse raciocínio (preferência) e tirar proveito dele.

Para o cálculo da determinação do grupo de preferência de um cliente, é utilizado um método de pontuação diferente do apresentado no MDP. De posse dos valores de tendência retornados pelo MCT é verificado se o valor subjetivo pertence a uma faixa de mais ou menos

X% (na simulação do SATYA foi utilizado o valor de 15%) de cada valor de tendência retornado pelo MCT. Caso o valor subjetivo esteja dentro da faixa, a métrica associada ao valor de tendência é acrescentada de um ponto. Caso contrário, a métrica associada recebe um valor zero. Estes valores de pontuação são armazenados em uma tabela denominada **Tabela de Preferência de Clientes** (TPC), também armazenada pelo SATYA.

Diferente de um provedor, a preferência de um cliente pode variar com o decorrer do tempo. A preferência de um provedor, por ser baseada nos valores efetivos de uso do serviço, possui uma baixa alteração, uma vez que esta pode ser determinada por uma característica especial do provedor (possui um melhor enlace de comunicação, por exemplo). Entretanto, um cliente pode variar a sua opinião de tempos em tempos, uma vez que a sua utilização dos serviços se dá de forma subjetiva. Para capturar alterações de avaliações fornecidas por clientes, a determinação da preferência do cliente não deve ser feita através da soma de todos os valores armazenados no vetor de elementos da TPC, mas de somente uma parte dela (no presente trabalho foi implementada a soma dos oito últimos valores).

É importante destacar também que não necessariamente um usuário avalia serviços diferentes sob os mesmos critérios. Como resultado, um mesmo usuário pode estar em mais de um grupo de preferência. Na versão atual do trabalho, a TPC vai conter os valores que refletem a preferência global do usuário em termos de avaliação, não sua preferência por tipo de serviço. Futuramente, serão feitas extensões ao mecanismo que associem preferências a tipos de serviços.

Quando um valor subjetivo não se encontra dentro da faixa de nenhum valor de tendência, podem ocorrer duas situações: (1) o SATYA pode estar com uma informação de monitoramento desatualizada ou (2) o usuário está com comportamento enganoso ou malicioso e nesse caso sua avaliação seria invalidada.

Para detectar a primeira situação, é investigado se o SATYA está com os parâmetros de QoS atualizados. Tal verificação é necessária, pois se o Monitor de Desempenho ficar ativamente enviando *probes* para avaliar um serviço, sua informação estará atualizada a custa de uma sobrecarrega no provedor, diminuindo seu desempenho. Para lidar com essa situação, é associado a cada valor de avaliação das métricas de QoS do Monitor de Desempenho um grau que informa o quanto sua informação está atualizada. Caso esse grau esteja abaixo de um limiar desejado, então a avaliação do Monitor de Desempenho ainda é considerada atualizada e sobraria apenas a opção de o usuário ser malicioso. Caso contrário deve-se ajustar a

freqüência de *probing* do Monitor de Desempenho de forma atualizar a informação de avaliação armazenada.

Baseado no sistema de pontuação para a determinação da preferência de clientes, podem ocorrer casos em que um cliente pertença a mais de um grupo de preferência ou a nenhum grupo de preferência. Um cliente ao acessar pela primeira vez um serviço não possuirá nenhum valor de preferência associado, sendo assim, não pertencerá a nenhum grupo de preferência. Com a utilização dos diversos serviços, será realizada a determinação e a conseqüente a alocação do cliente a um grupo específico. O mesmo acontece para a determinação dos grupos de preferência para provedores que ainda não forneceram nenhum serviço.

4.4.4 Módulo de Cálculo de Reputação

O Módulo de Cálculo de Reputação apresentado no Capítulo 3 é utilizado com a função disparar o processo de cálculo e armazenamento da reputação de provedores através do uso das avaliações subjetivas fornecidas por clientes do serviço. A reputação pode ser utilizada como uma medida auxiliar no processo de seleção de um serviço segundo um critério de QoS.

Quanto ao uso do Módulo de Cálculo de Reputação no SATYA, o cálculo da Reputação Individual de um fornecedor difere da calculada pelas avaliações utilizadas. A Reputação Individual é calculada utilizando as avaliações fornecidas pelos peers pertencentes ao mesmo grupo de preferência do peer, ao invés da Rede de Relacionamento do peer. Neste caso, pode ocorrer o problema do conluio, entretanto com a comparação dos valores objetivos obtido pelo Monitor de Desempenho e o possível descarte de avaliações feitas sem critério, tal problema é minimizado.

A Reputação Agregada, calculada utilizando todas as avaliações fornecidas pelos peers da rede, podem ser então utilizados por peers novos que ainda não pertençam a nenhum grupo de preferência, de forma a verificarem a reputação de um peer provedor quanto a confiabilidade em fornecer um serviço de acordo com as métricas de QoS publicadas.

4.5 Considerações Finais do Capítulo

Neste Capítulo o sistema de reputação proposto no Capítulo 3 foi estendido com novos módulos e aplicado a um cenário de Serviços Web que utiliza uma Arquitetura Orientada a Serviços. A extensão do Sistema de Reputação, que foi denominado de SATYA, teve os objetivos de aumentar a confiança no processo de descoberta e seleção de serviços através do uso dos valores de reputação, sem um aumento significativo na sobrecarga de monitoramento

na infra-estrutura de rede. Para realizar estes objetivos, o SATYA utilizou os valores objetivos obtidos pelas entidades de monitoramento denominadas Monitores de Desempenho e as avaliações fornecidas pelos clientes dos serviços.

A principal diferença na utilização do Mecanismo de Cálculo de Reputação no SATYA foi no cálculo da Reputação Individual dos peers provedores. Ao invés de utilizar os peers pertencentes à Rede Relacionamento do peer que requisita a reputação, foram utilizadas as avaliações fornecidas pelos peers pertencentes ao mesmo grupo de preferência do peer que requisitou a reputação. A utilização dos peers do mesmo grupo de preferência tem o objetivo de retornar um valor de reputação na métrica de grupo de preferência utilizado.

Sendo assim, os mecanismos apresentados no SATYA tiveram o objetivo de (i) diminuir o nível de subjetividade das avaliações fornecidas pelos clientes; (ii) prover valores de reputação que denotam a confiabilidade do provedor em fornecer o serviço de acordo com as métricas de QoS publicadas; (iii) criação de grupos de preferência de clientes que fornecem avaliações similares quanto ao uso dos serviços em uma determinada métrica de QoS e também, foram criados grupos de preferência de provedores de forma a agrupar provedores que fornecem um “melhor serviço” em uma determinada métrica de QoS. Além disso, os grupos de confiança criados podem então ser utilizados como mecanismo de incentivo para clientes fornecerem avaliações dos serviços.

O mecanismo que ajusta a freqüência de *probing* dinamicamente representa uma característica única em comparação com outros mecanismos de monitoramento que utilizam uma freqüência fixa. Ao adotar a freqüência dinâmica de *probing*, o SATYA possui a vantagem de aumentar a escalabilidade de todos o sistema em termos do número de mensagens de *probing* necessárias para manter as informações de QoS fornecidas pelos provedores atualizada.

No Capítulo 5, estão descritas as simulações realizadas, onde também se detalha o ambiente e as ferramentas utilizadas.

Capítulo 5 Simulações e Análise dos Resultados

Este Capítulo descreve as simulações realizadas para avaliação e verificação da validade da estratégia que foi adota na concepção do sistema de reputação proposto, conforme descrito nos Capítulos 3 e 4. É também apresentada a análise dos resultados das simulações.

Assim, este Capítulo está organizado em cinco seções. A Seção 5.1 descreve o ambiente de simulação utilizado, assim como, a integração da ferramenta de cálculo que utiliza Lógica Nebulosa. A Seção 5.2 apresenta as simulações realizadas com o Módulo de Cálculo de Reputação proposto no Capítulo 3, enquanto que na Seção 5.3 são descritas as simulações realizadas nos módulos de extensão SATYA detalhados no Capítulo 4. A Seção 5.4 finaliza o Capítulo apresentando as considerações finais.

5.1 Descrição Geral do Ambiente de Simulação

Para os testes dos módulos do sistema de reputação e da extensão SATYA, foram utilizados o simulador de redes Network Simulator (NS2) [52] e o simulador MATLAB. O NS2 fornece os mecanismos para criação de redes sem fio ou cabeadas, assim como primitivas para a troca de mensagens entre os diversos nós da rede a ser simulada.

A programação do NS2 é feita basicamente utilizando as linguagens C, C++ e OTcl. As linguagens C e C++ são utilizadas nos componentes internos do simulador, onde é necessário um intenso processamento. Já a linguagem de *script* OTcl é utilizada para o desenvolvimento dos *scripts* de simulação.

Como alguns dos módulos fazem uso da Lógica Nebulosa, utilizou-se o MATLAB. O MATLAB é composto por módulos para o desenvolvimento de aplicações específicas, como Redes Neurais, Sistemas Nebulosos, Mercado Financeiro, etc. O *Fuzzy Toolbox* é um módulo do MATLAB usado para o desenvolvimento de aplicações que utilizam Lógica Nebulosa.

O *Fuzzy Toolbox* é composto por um editor visual e de um programa para definição, configuração e execução de um sistema nebuloso. O editor visual permite a criação de todos os módulos de um sistema nebuloso, ou seja, definição dos conjuntos nebulosos para o processo de nebulização, as regras de inferência para o tratamento das variáveis lingüísticas e do método de desnebulização para obtenção dos valores escalares de saída. . O *Fuzzy Toolbox* armazena todas as informações de configuração em um arquivo no formato texto. Uma vez configurado o sistema nebuloso, para cada grupo de entradas escalares, o *Fuzzy Toolbox* utiliza um programa para executar o sistema nebuloso. Este programa foi escrito na linguagem C e que possui o código aberto, recebe como entradas o sistema nebuloso e as

variáveis escalares de entrada do sistema nebuloso, tendo como saída valores escalares do sistema nebuloso.

Para poder verificar o funcionamento do sistema nebuloso proposto nos ambientes de Rede Sem Fio Metropolitana e de Serviços Web, foi necessário integrar o programa Matlab de execução de sistemas nebulosos previamente configurado ao simulador de redes NS2. Esta integração consistiu na compilação deste programa no ambiente Linux e na execução de chamadas em tempo de simulação no NS2 através do comando *exec* da linguagem Otcl, no script de simulação. Este comando tem como função executar uma aplicação externa ao NS2 e obter os resultados em um *array* de *strings*.

Além dos *scripts* escritos em OTcl, também foram desenvolvidos alguns *scripts* na linguagem *Perl* com o propósito de organizar os resultados da simulação e calcular os parâmetros estatísticos, tais como, os valores médio, desvio padrão e intervalo de confiança dos resultados das simulações, os quais foram usados para a confecção dos gráficos. Para manter consistentes os parâmetros estatísticos calculados, foram realizadas 30 rodadas de simulação para cada configuração de teste, sendo o intervalo de confiança igual a 95%.

5.2 Avaliação do Módulo de Cálculo de Reputação

O objetivo principal desta avaliação foi verificar a eficácia da abordagem para minimizar o problema do conluio (anti-conluio) incorporada ao módulo MCR , comparando-a com a de outras duas abordagens já publicadas na literatura.

A estratégia da simulação foi considerar que o peer cliente (aquele que sofre o ataque de conluio) sempre teria um valor médio de reputação alto no uso de serviços na ausência de ataque. Também considerou-se que os peers maliciosos (em conluio) sempre procuravam reduzir a reputação do peer vítima, de forma que os serviços solicitados por estes fossem negados devido a baixa reputação. Adicionalmente, para verificar a eficácia da proposta de combate ao conluio, foram também realizadas simulações para os mecanismos anti-conluio propostos em [7, 8] nos mesmos cenários.

Assim, para as três abordagens anti-conluio, foi monitorado durante as simulações o decaimento dos valores de reputação do peer vítima e o número de serviços solicitados pelo peer vítima não atendidos devido à queda de seu valor de reputação.

O cenário adotado neste teste foi o de uma Rede Metropolitana Sem Fio (RMSF) e de uma infra-estrutura de comunicação P2P. Entretanto, não foi necessário implementar no NS2 as primitivas de comunicação da RMSF e da rede P2P, uma vez que as simulações realizadas tiveram o objetivo de avaliar o mecanismo no nível de aplicação. Quanto à conectividade dos

nós da rede em nível de enlace, adotou-se o padrão de rede sem fio 802.11 com uma única área de cobertura de 100x100 metros com 60 nós, de maneira que a conectividade entre todos os nós/peers fosse garantida.

5.2.1 Variação da Reputação Agregada de um Peer Cliente sob Ataque de Conluio

Para a avaliação do MCR, foi configurado um nó da rede como um peer cliente (vítima), um nó como um peer da Rede de Reputação (armazena a reputação) e os nós restantes como peers provedores. No início da simulação, um grupo de peers provedores é escolhido de forma aleatória para atuarem como peers em conluio com o objetivo de diminuir a reputação do peer cliente.

A partir do momento que um peer da Rede de Reputação recebe um valor de reputação para armazenar na sua Tabela de Reputação Agregada (TRA), este deve realizar um teste para verificar se tal valor está dentro do padrão de distribuição de freqüência dos valores de reputação que o peer cliente recebeu previamente (histórico). Caso não esteja dentro do padrão de distribuição, este valor é descartado no processo de atualização da Reputação Agregada. Entretanto esse valor é registrado em uma base de valores históricos de avaliação do peer cliente, para fins de atualização dos valores usados no cálculo da distribuição. Foram configurados os seguintes valores como parâmetro do padrão de distribuição de freqüência: 50%, 75%, 85% e 95%. Um valor de 95% configurado como parâmetro na distribuição de freqüência compreende a verificação se o novo valor de avaliação recebido pertence ao intervalo de 95% dos últimos valores de avaliação recebidos para não ser descartado.

Caso o valor de avaliação recebido esteja dentro do padrão de distribuição, a reputação do peer cliente será atualizada conforme a fórmula da Figura 26, que foi apresentada no Capítulo 3. Na avaliação do MCR, realizou-se a comparação da evolução dos valores de reputação do peer cliente sob ataque de conluio para as propostas apresentadas em [7, 8], os quais utilizam valores fixos para o parâmetro α da fórmula da Figura 26 e não verificavam o padrão de distribuição de valores de reputação recebidos pelos peers clientes.

$$Rep_{peer} = \alpha * Rep_{média} + (1-\alpha) * Ava_{nova}$$

Figura 26 – Fórmula para evitar oscilações na atualização da Reputação Agregada

Os gráficos da Figura 27 e Figura 28 mostram a variação do valor da Reputação Agregada do peer cliente, armazenada na TRA no peer da Rede de Reputação, em função do percentual de peers em conluio em relação ao número de peers total na rede. O gráfico da Figura 27 refere-se a abordagem utilizada na presente proposta que utiliza a distribuição de freqüências e quantifica os valores de α dinamicamente. Já o gráfico da Figura 28, além de

não utilizar a distribuição de freqüências, especifica um α de valor fixo de 0,95, conforme utilizado nos trabalhos [7, 8]. O valor da Reputação Agregada inicial do peer cliente foi configurada em 0,5, e simulada somente a utilização de uma classe de serviço.

A taxa de requisição de serviços do peer cliente foi configurada em uma requisição por segundo e o tempo total de simulação em 3000 segundos. Durante os primeiros 300 segundos de simulação, não ocorriam ataques de conluio. Entretanto, passados os 300 segundos, os peers em conluio começavam a afetar a reputação do peer cliente, informando valores de avaliação entre Muito Baixo ou Baixo (intervalo [0, 0.4]), com relação ao fornecimento do serviço, caso fossem acessados. Quando no fornecimento de um serviço de um peer provedor não integrante do grupo do conluio, o valor de avaliação fornecido por este era entre Alto ou Muito Alto (intervalo [0.6, 1.0]).

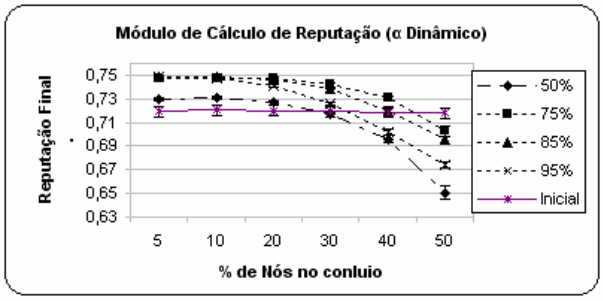


Figura 27 – Atualização da TRA com a variável α dinâmico

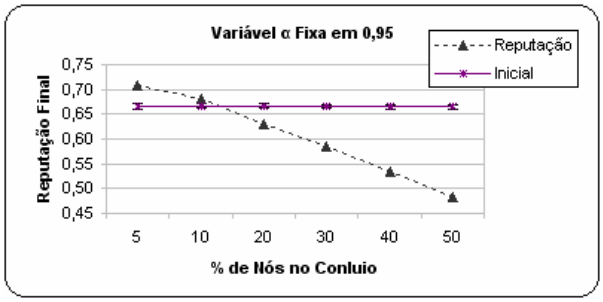


Figura 28 – Atualização da TRA com a variável α fixa em 0,95

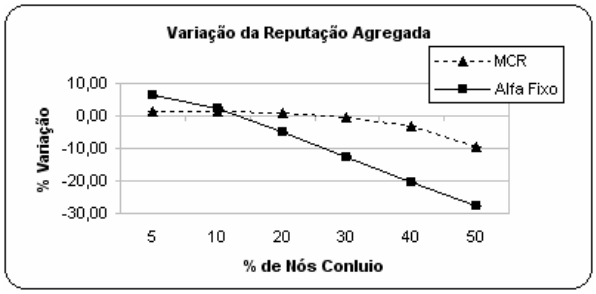


Figura 29 – Variação do valor da Reputação Agregada de um peer cliente

O gráfico da Figura 27 mostra as curvas referentes ao valor médio da Reputação Agregada do peer cliente, calculada pelo MCR, utilizando os valores de 50%, 75%, 85% e 95% como parâmetro da distribuição de freqüência. É também apresentada uma curva (linha contínua) com o valor médio inicial da Reputação Agregada do peer cliente antes da existência de grupo de peers em conluio (isto é, ao final do período inicial de simulação de 300 segundos).

Ao comparar as curvas da Figura 27, constata-se que até a formação de um grupo em conluio de aproximadamente 25% dos nós da rede, a Reputação Agregada do peer cliente se manteve em um patamar acima do valor médio inicial da Reputação Agregada medido após o período de 300 segundos. Isto indica que o mecanismo para minimizar o problema do conluio

incorporado ao MCR foi efetivo para qualquer valor de distribuição de freqüência. Entretanto, constata-se que a partir de aproximadamente 45% de nós em conluio, o mecanismo não obteve sucesso no combate ao conluio, pois os valores de Reputação Agregada final tornaram-se inferiores em relação ao valor inicial antes do conluio.

Vale ressaltar que o menor valor de reputação apresentado pela curva com parâmetro de 50% em relação à curva de 95% na Figura 27 se deve a distribuição de freqüências de ocorrência de valores variar ao longo da simulação. Ao final do período inicial de simulação, a freqüência de ocorrência de valores elevados de avaliação é alta, devido à ausência de ataque de conluio. À medida que a simulação configurada com o parâmetro 50% de distribuição de freqüência progride, a Reputação Agregada não é atualizada para um grande número de avaliações, sendo estas avaliações lícitas ou não. Isto faz com que o seu valor permaneça relativamente constante, o que evita considerar as avaliações maliciosas (oriundas do grupo de conluio) no cálculo da Reputação Agregada. Entretanto, todos os valores de avaliação são incluídos na atualização da distribuição de freqüência, o que, com o passar do tempo, faz com que esta distribuição passe a apresentar uma concentração crescente de valores baixos de avaliação oriundos dos peers pertencentes ao grupo de conluio. Em um determinado momento da simulação, o MCR passa também a aceitar valores baixos de avaliação (avaliações maliciosas) para o cálculo de reputação. Assim, ao longo da simulação, a reputação tem uma tendência maior de queda para a configuração da distribuição de freqüências de 50% do que a de 95%. Neste caso (95%), apesar de todos os valores de avaliação também serem considerados na atualização da distribuição de freqüência, o MCR considera no cálculo da reputação tantos os valores de avaliação altos quanto baixos, produzindo um valor de reputação mais alto do que no caso anterior (50%).

O gráfico da Figura 28 mostra a variação da reputação em função do percentual de peers em conluio com parâmetro α fixo em 0,95. Os valores referentes a este gráfico foram obtidos nas mesmas rodadas de simulação para obtenção dos resultados referentes ao gráfico da Figura 27. Também é apresentada na Figura 28 a curva (linha contínua) representando o valor da Reputação Agregada média do peer cliente, antes da formação dos peers em conluio.

Ao comparar a duas curvas do gráfico, constata-se que o valor da Reputação Agregada começa a decair a partir da formação de um grupo de conluio com tamanho de aproximadamente 12%. As curvas da Figura 27 mostram que o decréscimo da Reputação Agregada final com o aumento do número de peers em conluio é bem menos acentuado se comparado com o da Figura 28. Isto demonstra a eficácia dos usos do processo de distribuição

de freqüência e do parâmetro α configurado dinamicamente de acordo com os valores de relacionamento e reputação com o peer cliente.

O gráfico da Figura 29 é uma composição da curva Figura 27 referente ao parâmetro de distribuição de freqüência igual a 75% e a curva da Figura 28 que utiliza o parâmetro α fixo em 0,95, excetuando o fato que, em vez de se utilizar o valor absoluto de reputação, utilizou-se, no eixo das ordenadas, o percentual de variação em relação ao valor de reputação no final do período inicial de simulação (período inicial de 300 segundos). Comparando as duas curvas da Figura 29, referentes a abordagem do presente trabalho e aquelas dos trabalhos relacionados, observa-se que, a curva referente ao mecanismo proposto (MCR) apresenta uma queda mais suave, com um valor médio final de Reputação Agregada negativa de 9% aproximadamente para um grupo de conluio com 50% dos peers. Tal fato deve-se a proposta apresentada nesse trabalho adotar descarte antecipado de valores (distribuição de freqüência) e atualizar a tabela de reputação utilizando um α proporcional ao nível de relacionamento entre os peers. Em suma, a proposta de atualização da TRA usando o MCR é mais resiliente do que as propostas apresentadas nos trabalhos anteriores mencionados.

5.2.2 Quantidade de Serviços Acessados pelo Peer Cliente sob Efeito de Ataque de conluio

A Figura 30 e a Figura 31 apresentam dois gráficos representando a quantidade de serviços requisitados e realizados com sucesso por um peer cliente sofrendo, ataques de conluio. O gráfico da Figura 30 mostra a quantidade de acessos fornecidos por um peer provedor que fornece serviços para clientes com valores de Reputação Agregada maiores ou iguais a 0,5. Caso o peer cliente não possua o valor mínimo de 0,5, o fornecimento do serviço é negado. O gráfico da Figura 31 corresponde ao caso em que o peer provedor fornece o serviço somente quando o peer cliente tem um valor de Reputação Agregada mínima de 0,7. Nesta simulação, somente são computados os acessos aos serviços que não pertencem a peers provedores que estão em conluio, uma vez que os peers provedores em conluio foram configurados para sempre fornecerem o serviço e retornar um valor baixo de uso do mesmo. Todos os valores de taxa de aceitação de serviços usando o MCR foram obtidos para uma distribuição de freqüência igual a 75%.

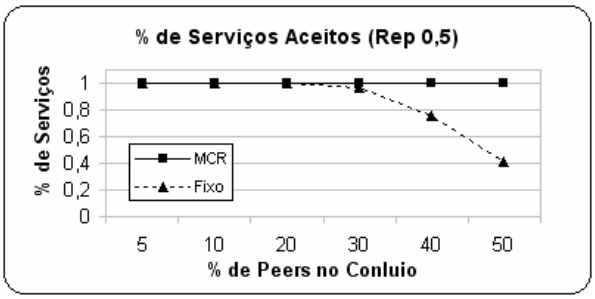


Figura 30 – Porcentagem de serviços aceitos com Reputação Agregada mínima de 0.5

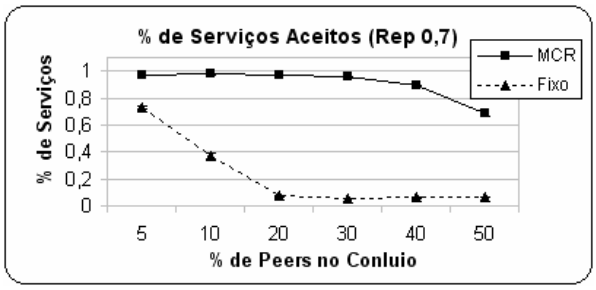


Figura 31 – Porcentagem de serviços aceitos com Reputação Agregada mínima de 0.7

O gráfico da Figura 30 mostra duas curvas, uma de linha contínua e outra de linha pontilhada, que correspondem respectivamente a abordagem proposta neste trabalho (o parâmetro α sendo configurado dinamicamente e o uso da distribuição de freqüências) e os métodos que usam o parâmetro α fixo. Comparando as duas curvas, constata-se a eficácia da abordagem que minimiza o problema do conluio proposta, assegurando, dentro do escopo da simulação, a aceitação de todas as requisições do peer cliente independentemente do tamanho de grupo de conluio. Isto significa que o MCR obteve sucesso em manter os valores de Reputação Agregada superiores a 0,5 apesar de os peers em conluio atuarem ao longo da simulação no sentido de reduzir as avaliações do peer cliente com o objetivo de ter seus serviços negados pelos peers servidores. Nota-se claramente na Figura 30 a queda acentuada de eficácia das outras abordagens anti-conluio (curva com linha pontilhada) a partir de tamanhos de grupos em conluio iguais a 30 % dos peers. Com um grupo de conluio de 30% do total de peers provedores, houve em torno de 3% de acessos a serviços negados, e com um tamanho de 50%, um total de 60% de acessos negados.

A Figura 31 apresenta curvas similares às curvas da Figura 30, só que com o valor mínimo de aceitação de requisições de serviços configurado em 0,7. Apesar de todas as abordagens terem sofrido redução significativa de eficácia, é fácil perceber que a eficácia da abordagem proposta (curva com linha contínua) permaneceu superior em comparação com a abordagem relacionada (linha pontilhada), inclusive a discrepância entre elas aumentou devido ao forte acréscimo da taxa de negação de acessos quando se utilizaram as abordagens dos trabalhos relacionados. Em outras palavras, o MCR proporcionou uma queda mais suave na taxa de negação de acesso a serviços do que do que naquelas observadas nos trabalhos relacionados [7, 8]. Só para se ter uma noção comparativa entre as abordagens, observa-se que, para um grupo de conluio de 30% do total de peers provedores, a taxa de aceitação de serviços gerados pelo peer cliente foi superior a 95% com o uso do MCR, enquanto que, sem

a utilização do MCR, para uma taxa de 20% de peers provedores em conluio, o peer cliente teve em média 93% dos seus acessos negados.

Também foram realizados testes para medir as taxas de aceitação de serviços de peers provedores que exigiam Reputação Agregada dos peers clientes com valores mínimos de 0,3, 0,4, 0,6 e 0,8. Para o valor mínimo de 0,3, a taxa de aceitação foi de 100% utilizando o MCR ou não, indicando que o MCR não impede que peers clientes com baixos valores de Reputação Agregada acessem serviços de peers provedores que exigem valores de reputação mínimos muito baixos. Esta característica do MCR é muito importante, pois evita que acessos legítimos a serviços que não necessitam de alto grau de segurança sejam negados. A Tabela 6 mostra o resultado dos cenários configurados com as taxas 0,4, 0,6 e 0,8 mínimas para fornecer o serviço.

Tabela 6 – Valores de Taxa de Aceitação de Serviços para Diversos Cenários

Abordagens	Valores de Reputação Mínimos Simulados		
	0,4	0,6	0,8
Com MCR	100@50	98@50	1@5 0@>5
Sem MCR	98@50	16@50	0@≥5

O formato dos valores de taxa de aceitação da Tabela 6 é do tipo X@Y, onde X é o próprio valor da taxa de aceitação e Y é o percentual do total dos peers que atuam em conluio durante as simulações, ou seja, corresponde ao tamanho do grupo de peers em conluio. A Tabela 6 permite se ter uma idéia geral da eficácia da abordagem utilizando o MCR proposta em termos quantitativos, mostrando o limite de aplicação da abordagem proposta diante dos cenários escolhidos. Para valores de reputação de 0,8, por exemplo, todas as solicitações de serviços foram rejeitadas (0@>5) para grupos em conluio com número de peers maior que 5% do total de peers. Isto acontece porque serviços deste tipo requerem que os peers clientes sejam bastante confiáveis por se tratarem de serviços críticos em termos de segurança.

5.3 Avaliação dos Módulos do SATYA

Nesta Seção são descritas as simulações realizadas com o intuito de avaliar os módulos presentes no SATYA, apresentados no Capítulo 4. As simulações foram conduzidas para avaliar o comportamento dos mecanismos adotados no SATYA no contexto de Serviços Web e, como trabalho futuro, é sugerida a implementação de uma versão completa do

SATYA para utilização em um ambiente real de Serviços Web a fim de demonstrar plenamente todos os benefícios que podem ser obtidos com o sistema.

Primeiramente na Seção 5.3.1 serão apresentadas as simulações realizadas para a avaliação dos módulos do SATYA integrados a um Agente de Serviços. Na Seção 5.3.2 é detalhado o uso dos grupos de preferência na avaliação do grau de satisfação dos peers clientes no uso dos serviços, enquanto que na Seção 5.3.3 é apresentado um benefício adicional ao SATYA que é a possibilidade de realizar um balanceamento de carga de serviços fornecidos pelos peers provedores. Por fim, na Seção 5.3.4 são apresentadas as simulações realizadas para a avaliação do uso da reputação no processo de descoberta de serviços.

Nas simulações utilizou-se o simulador de redes NS2, sendo que a infra-estrutura de rede utilizada foi uma rede cabeada com um total de 60 nós configurados como provedores ou clientes. Mais uma vez, não houve a necessidade da implementação da rede P2P sobreposta à infra-estrutura de rede, uma vez que as simulações foram realizadas em nível de aplicação.

Uma vez configurada infra-estrutura de rede, para implementar o modelo de falhas das métricas de QoS dos serviços fornecidos (exceto dos resultados da Seção 5.3.4), foi utilizada uma distribuição de Bernoulli, no qual um provedor possui 98% de chances de entregar um serviço respeitando as métricas de QoS publicadas. Foram realizadas 30 rodadas de simulação, sendo em seguida obtidos os valores médio, desvio padrão e intervalo de confiança de 95%.

5.3.1 Avaliação do SATYA

O objetivo das simulações desta Seção é comprovar que o uso dos mecanismos do SATYA efetivamente provê um valor de avaliação das métricas de QoS publicadas de um provedor e que reflita o seu estado atual, ao mesmo tempo em que diminui a necessidade de realização de *probings*. Nas simulações, a disposição dos nós foi estabelecida da seguinte forma: do total de 60 nós, 1 nó foi configurado como peer provedor, 1 nó como peer Monitor de Desempenho e Agente de Serviço, e os outros 58 nós foram configurados como peers clientes. Para atingir a meta dessa simulação, o mesmo cenário foi rodado, primeiramente, sem a utilização do SATYA e em seguida com o SATYA ativado. A Figura 32 apresenta os resultados das simulações realizadas com o SATYA desativado.

Os valores obtidos sem a utilização do SATYA foram utilizados como valores bases para comparação. Esses valores foram obtidos da seguinte forma: inicialmente o peer cliente envia uma requisição ao Agente de Serviço informando o serviço que deseja utilizar. O Agente de Serviço retorna o valor objetivo sem tendência do peer provedor atualmente

armazenado. Em seguida, o peer cliente utiliza o serviço do peer provedor obtendo os valores efetivos das métricas de QoS relativos a utilização do serviço. Cabe mencionar que tais valores efetivos refletem o estado atual do peer provedor, conhecido na simulação, mas que não está disponível para o SATYA no mundo real.

Nesse ponto, calcula-se um novo valor de avaliação objetiva sem tendência baseado no valor efetivo de QoS obtido através da utilização do serviço. Calcula-se, então, a diferença entre esse valor e a avaliação objetiva sem tendência fornecida pelo monitor. Conforme apresentado na Figura 32, para representar diferentes limiares de atualização dos valores de QoS armazenados no monitor, foram criadas três faixas (2%, 4% e 10%), representadas por três curvas. Por exemplo, para a faixa de 2%, o valor armazenado no monitor é considerado atualizado somente se a diferença entre o valor recuperado do monitor e o valor efetivo for menor ou igual a 2% (do valor efetivo). No gráfico da Figura 32 o eixo das ordenadas fornece uma medida, nomeada taxa de acerto, que reflete em termos porcentuais o grau de atualização do monitor, ou seja, o quanto os valores armazenados são próximos dos valores efetivamente obtidos no uso do serviço. Um valor de 1 (ou 100%) indica que em todas as requisições o valor armazenado correspondia ao valor efetivo. Foram simulados cinco intervalos de envio de mensagens de *probing* (5, 10, 20, 30 e 60 segundos). A taxa de requisição de serviços foi mantida constante em 1,5 requisições por segundo.

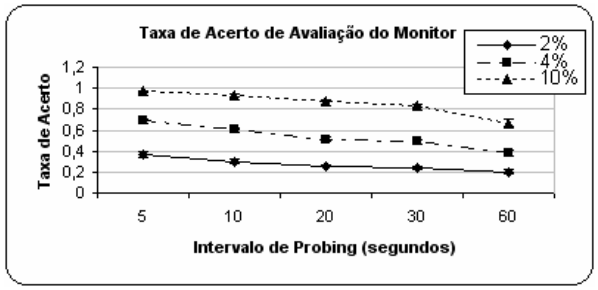


Figura 32 – Taxa de Acerto – Sem o uso SATYA

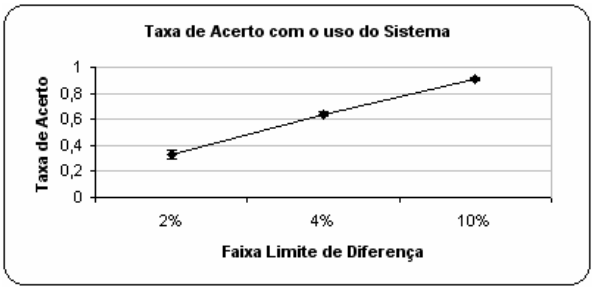


Figura 33 – Taxa de Acerto – Com o uso do SATYA

Conforme mostra a Figura 32, as taxas de acerto em todas as faixas de valores limites apresentam uma queda conforme o intervalo de probing é aumentado. Este fato é conseqüência do aumento do intervalo de tempo de envio de requisições para monitoramento. Considerando a faixa de valores limites de 10%, com um intervalo de monitoramento de 5 segundos, a taxa de acerto é de aproximadamente 97%, isto é, em 97% dos casos em que foram avaliados o valor armazenado no monitor com o valor efetivo de QoS do serviço, estes valores foram considerados como sendo atualizados. Analisando a faixa de 2%, este valor cai para 37%.

A Figura 33 apresenta os valores de taxa de acerto obtidas com o SATYA ativado, para as faixa de valores limites de 2%, 4% e 10%. Os eixos do gráfico não apresentam a freqüência de monitoramento já que esta é variável quando o SATYA está ativado. Para analisar o comportamento do SATYA, os valores da curva apresentada no gráfico da Figura 33 foram comparados com os valores do gráfico da Figura 32, considerando o intervalo de *probing* de 5 segundos. Esse intervalo foi escolhido uma vez que este representa o pior caso (maior freqüência de requisição) para o SATYA (valores de QoS mais atualizados). Os resultados mostraram que, para a faixa de 2%, a taxa de acerto é, aproximadamente, 37% sem a utilização do SATYA, enquanto que com a utilização do SATYA este valor é de 33%. Para valores de faixa de 4% e 10%, as respectivas taxas de acerto, para o caso sem o SATYA, são de 69% e 97%, enquanto que com a utilização do SATYA, os valores são de 64% e 91%. Logo, as taxas de acerto obtidas com o SATYA são próximas ao que se obtêm sem o SATYA e com o monitor utilizando uma alta freqüência de probing.

O passo final dessa simulação é verificar a possível redução do número de mensagens de monitoramento enviadas por parte do monitor quando o SATYA está em funcionamento. A Figura 34 mostra uma curva com a relação entre o número de mensagens de *probing* geradas pela entidade monitora com o SATYA ativado e o número de mensagens de *probing* com o SATYA desativado e com um intervalo de *probing* de 5 segundos. Para uma faixa limite de 2%, com o SATYA ativado, são enviadas aproximadamente 38,6% de mensagens somente, comparadas com o total de mensagens enviadas com o SATYA desativado. Para as outras faixas limite (4% e 10%) essa relação é ainda mais favorável (21% e 12%). Esses números demonstram que o SATYA provê uma solução altamente escalável sem deterioração da corretude da avaliação.

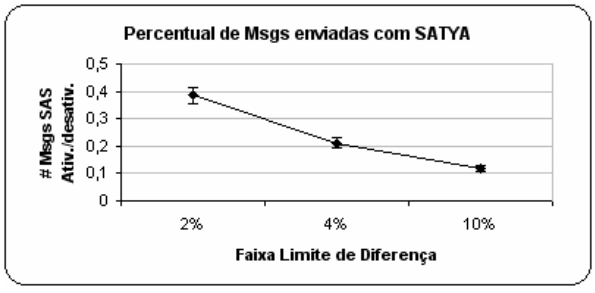


Figura 34 – Percentual de mensagens com SATYA

5.3.2 Avaliação do uso de Grupos de Preferência

O segundo conjunto de simulações tem como objetivo avaliar o benefício do mecanismo de criação de grupos de preferência do SATYA. Outro objetivo das simulações consiste em avaliar o benefício da utilização do mecanismo para a criação de grupos de

preferência. Para tal, foram comparadas as avaliações fornecidas por peer clientes ao utilizar peer provedores do mesmo grupo de preferência, com avaliações fornecidas por peer clientes utilizando peer provedores de diferentes grupos de preferência, inclusive do seu próprio grupo. Nessa simulação, do total de 60 nós disponíveis, 10 nós foram configurados como peers provedores e o restante como peers clientes. Para analisar o efeito da utilização de grupos de preferência no SATYA foram geradas duas curvas, uma representando a escolha de provedores de modo aleatório, isto é, de qualquer grupo de preferência, e outra representando escolha de provedores do mesmo grupo.

Na Figura 35 é mostrada a média das avaliações subjetivas fornecidas pelos peers clientes, sobre os serviços utilizados de peers provedores do mesmo grupo de preferência ("Mesmo Grupo") e de diferentes grupos de preferência ("Aleatório"), com respeito a diferentes taxas de requisição de serviços. Nota-se que a média de valores de avaliações subjetivas é maior quando são utilizados provedores do mesmo grupo de preferência em todos os valores de taxa de requisição. A utilização de serviços de peers provedores do mesmo grupo de preferência implica melhores avaliações fornecidas por peers clientes e, por conseqüência, provável melhor oferta de serviço. Entretanto, notou-se que a utilização de serviços de provedores que pertençam ao mesmo grupo de preferência resulta em um maior número de violações dos parâmetros de SLAs por parte dos provedores. Esse fato é decorrente da redução na quantidade de provedores disponíveis que podem ser utilizados pelo cliente.

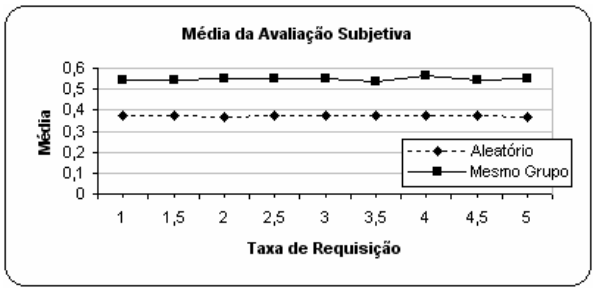


Figura 35 – Média da avaliação subjetiva final de todos os serviços consumidos

5.3.3 Avaliação dos benefícios do Balanceamento de Carga dos Peers Provedores

O objetivo desta fase de simulações é avaliar os benefícios que o uso do balanceamento de carga quando na seleção de peers provedores pertencentes do mesmo grupo de preferência do peer cliente. Nesta fase foi adotado o mesmo cenário utilizado da Seção 5.3.2, e foram utilizadas três taxas de requisição de serviços de forma a comparar a escalabilidade do sistema: Alta, Intermediária e Baixa. A taxa de requisição de serviço considerada Alta foi configurada com o valor de 8 requisições por segundo (req/seg), a taxa de requisição Intermediária de 4 req/seg, e a taxa de requisição Baixa em 1.5 req/seg.

O mecanismo de balanceamento de carga quando na escolha de serviços de peers provedores foi simulado da seguinte forma: sempre quando um peer cliente requisita um serviço, o SATYA retorna um peer provedor com a menor taxa de fornecimento de serviços no instante da requisição. O balanceamento de carga é sempre realizado dentro do mesmo grupo de preferência de peers provedores e clientes, isto é, o peer provedor selecionado será o que tiver a menor taxa de fornecimento de serviço em um intervalo de tempo e que pertença ao mesmo grupo de preferência do peer cliente.

Sendo assim, os experimentos realizados para avaliar o mecanismo de balanceamento de carga foram baseados através da avaliação do grau de satisfação dos clientes no acesso dos serviços com e sem a utilização do mecanismo. O grau de satisfação de um cliente reflete a quantidade de serviços acessados no qual não ocorreram violações das métricas de QoS publicadas pelo provedor. O número de peers provedores e peers clientes variavam durante as simulações e três métricas de QoS foram utilizadas: Tempo de Resposta, Disponibilidade e Desempenho. Considerando as três métricas de QoS utilizadas, foram definidos três grupos de preferência (um para cada métrica), sendo que cada peer cliente foi configurado para pertencer a um determinado grupo. O número de peers provedores pertencentes a cada grupo de preferência variava de 2 até 5 (resultando em um total de 6 até 15 peers provedores na rede).

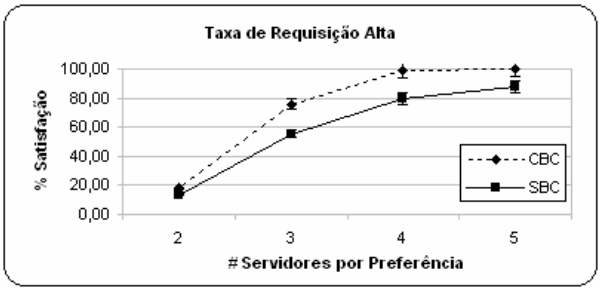


Figura 36 – Porcentagem de Serviços Negados: Taxa de Requisição Alta

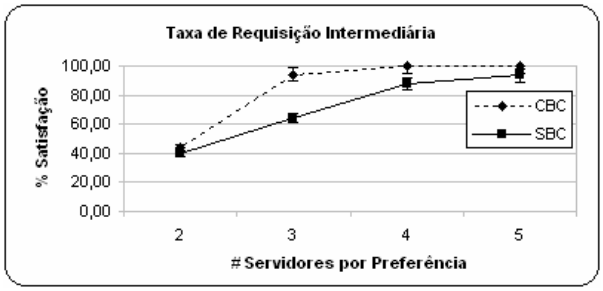


Figura 37 – Porcentagem de Serviços Negados: Taxa de Requisição Intermediária

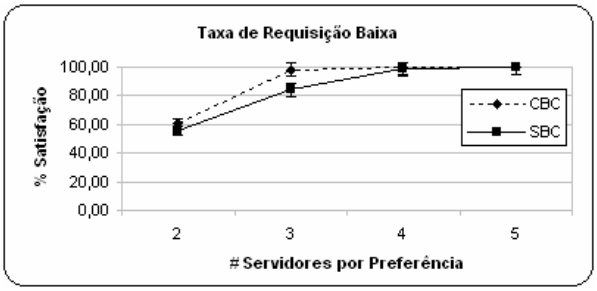


Figura 38 – Porcentagem de Serviços Negados: Taxa de Requisição Baixa

As Figuras 36, 37 e 38 apresentam a porcentagem do grau de satisfação dos clientes para cada taxa de requisição de serviços simulada (Alta, Intermediária e Baixa). Uma redução

significativa foi conseguida com a adoção do mecanismo de balanceamento de carga. Os benefícios obtidos com o uso deste mecanismo foram resultados da adição de informações no Agente de Serviços a respeito da carga de cada peer provedor em um dado intervalo de tempo e o uso destas informações no processo de atendimento de uma requisição.

Por exemplo, no cenário simulado da Figura 36, com três peers provedores em cada grupo de preferência e com uma taxa Alta de requisição de serviços, a porcentagem do grau de satisfação foi de aproximadamente 22,3% maior com o uso do mecanismo de balanceamento de carga (CBC) do que sem o seu uso (SBC). Com o uso de quatro peers provedores em cada grupo de preferência, esta diferença diminui para 19,4% (Figura 36).

Estes resultados obtidos demonstram que o uso do mecanismo de balanceamento de carga para a distribuição das requisições feitas pelos peers clientes entre os peers provedores dentro de um mesmo grupo de preferência aumenta o número de fornecimento de serviços sem desrespeitar as métricas de QoS publicadas, resultando em um melhor uso dos recursos disponíveis.

5.3.4 Uso do SATYA no Processo de Descoberta de Serviços

Os experimentos realizados nesta quarta fase de simulações do SATYA possuem o objetivo de analisar como o comportamento de um peer provedor influencia o valor de reputação do mesmo. Este valor de reputação pode ser utilizado como um indicador da freqüência que um peer provedor respeita as métricas de QoS publicadas. No processo de descoberta de peer provedores com a utilização do SATYA, a escolha de um peer provedor pode levar em consideração: (i) os valores de métricas de QoS publicadas; (ii) os valores de reputação dos peers provedores; (ii) ou ambos. A reputação de um peer provedor denota o quanto este efetivamente fornece os serviços dentro dos valores de QoS publicados. Portanto, com uso do SATYA no processo de descoberta de serviços, um peer cliente terá a possibilidade de selecionar peer provedores que possuem (i) a melhor métrica de QoS desejada (por exemplo, o peer provedor que fornece o serviço com o menor Tempo de Resposta); (ii) o maior valor de reputação em uma métrica de QoS; (iii) ou a melhor relação entre o valor de reputação e o da métrica de QoS publicada.

Nesta fase de simulação, foi adotado o cenário com 60 nós e valores de taxa de requisição de serviços (Alta, Intermediária e Baixa) iguais aos que foram configurados na Seção 5.3.3. O mecanismo simulado para um peer cliente selecionar um peer provedor compreende os seguintes passos: (i) seleção de um serviço a partir do conjunto de serviços disponíveis; (ii) escolha de uma métrica de QoS (por exemplo, Tempo de Resposta); (iii)

determinação dos requisitos das métricas de QoS (por exemplo, peers provedores com Tempo de Resposta menores que 1000 ms); (iv) execução do método **RetornaProvedores**, o qual retorna uma lista de peers provedores que satisfazem os requisitos das métricas de QoS (neste caso, todos os peers provedores que possuem publicadas a métrica Tempo de Resposta menor que 1000 ms); (v) uma vez recebida a lista de peers provedores, executa o método **SelecionaProvedores**, que determina o melhor peer provedor a ser usado dado os requisitos de QoS.

Uma vez selecionado um peer provedor, o peer cliente poderá requisitar o serviço através da execução do método **ExecutaServiço**. O método **ExecutaServiço** simula um peer provedor fornecendo uma requisição de serviço dentro de um contexto corrente de execução, o qual varia dinamicamente dependente de uma série de fatores que influência diretamente a capacidade deste em fornecer o serviço de acordo com as métricas de QoS publicadas.

Para a modelagem do comportamento de fornecimento de um serviço de um peer provedor, foi utilizado um processo de Bernoulli. De acordo com este modelo adotado, um peer provedor possui 90%, 80%, 70%, 60% e 50% de capacidade (probabilidade) de fornecer o serviço requisitado de acordo com as métricas de QoS publicadas. A Figura 39 mostra os resultados obtidos. O eixo das abscissas denota a capacidade do peer provedor fornecer o serviço de acordo com as métricas de QoS publicadas e o eixo das ordenadas mostra a Reputação Agregada média final dos peers provedores. De acordo com os resultados obtidos da Figura 39, a Reputação Agregada média final do peer provedor apresenta um queda linear proporcional a sua capacidade de cumprir as métricas de QoS publicadas. Esta queda ocorre uma vez que baixos valores de reputação são atribuídos durante a simulação para peers provedores que não cumprem as métricas de QoS publicadas. De acordo com o gráfico da Figura 39, os valores de reputação realmente refletem quão confiáveis as métricas de QoS publicadas por um peer provedor são.

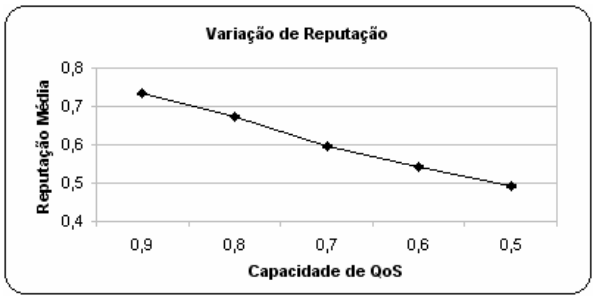


Figura 39 – Variação da Reputação de acordo com o desempenho das métricas de QoS do peer provedor

A última etapa da simulação tem o objetivo de comparar o uso ou não do SATYA, isto é, avaliar o fornecimento ou não dos valores de reputação em conjunto com as métricas de QoS publicadas. Agentes de Serviços tradicionalmente não fornecem os valores de reputação agregados ás métricas de QoS, de forma que os peers clientes somente saberão se o peer provedor cumpre as métricas QoS publicadas após o seu uso. Quando do uso de um Agente de Serviço integrado com o SATYA, o acréscimo dos valores de reputação às métricas de QoS publicadas provê aos peers clientes a capacidade de melhor selecionarem o peer provedor.

Sendo assim, nesta etapa da simulação do SATYA será comparado um Agente de Serviços integrado com o SATYA com um Agente de Serviços tradicional, com respeito à porcentagem de valores de métricas de QoS que não foram cumpridas. Para esta etapa da simulação, o seguinte ambiente foi implementado: do total de 60 nós, 10 foram configurados como peers provedores e o restante como peers clientes. Todos os peers provedores foram configurados para fornecerem o mesmo tipo de serviço e publicarem os valores das métricas de QoS referentes a mesma métrica. A taxa de requisição de serviços foi configurada em 5 req/seg.

Em um Agente de Serviços tradicional sem o SATYA integrado, todos os peers provedores (aqueles que cumprem ou não as métricas de QoS publicadas) possuem a mesma probabilidade de serem escolhidos, uma vez que estes cumprem o requisito desejado pelo peer cliente. O impacto negativo da presença de peers provedores não confiáveis refletem no grau de insatisfação dos peers clientes. De outra forma, com o SATYA integrado ao Agente de Serviços, o processo de escolha de peers provedores utiliza tanto as métricas de QoS publicadas quanto os valores de reputação associados. Dessa maneira, peers provedores que não cumprem os valores de métricas de QoS publicadas irão receber um baixo valor de reputação, resultando em uma baixa probabilidade de estes serem escolhidos por outros peers clientes ao longo do tempo.

Nas simulações, os peers clientes foram configurados individualmente com um critério aleatório de escolha de serviços. Foram implementados três critérios: (i) maior valor de reputação; (ii) “melhor” valor de métrica de QoS publicada (dependente do tipo de métrica QoS, por exemplo, o menor tempo de resposta; (iii) um valor médio entre o maior valor de reputação e o “melhor” valor de métrica de QoS publicada. O critério aplicado pelo peer cliente era executado na escolha de um peer provedor dentro da lista de peers provedores retornada pela execução do método **SelecionaProvedores**. A Figura 40 mostra a porcentagem de ocorrência de métricas de QoS violadas com e sem o uso dos SATYA. O eixo das

abscissas denota a quantidade de peers provedores que cumprem a QoS publicada (portanto, provedores confiáveis) em cada rodada de simulação, e o eixo das ordenadas denota a porcentagem de QoS violadas.

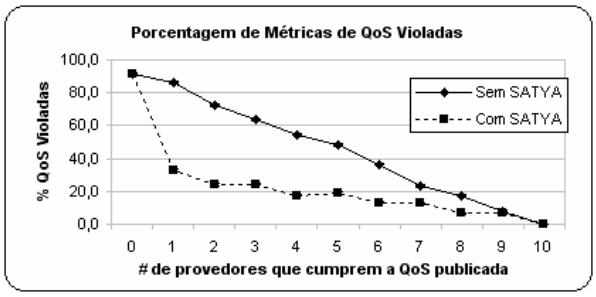


Figura 40 – Porcentagem de métricas de QoS violadas

De acordo com a Figura 40, a ausência de peers provedores resulta em um grande número de violações de QoS (aproximadamente 91,3% sem o SATYA e 91,0% com), gerando um baixo valor de satisfação para com os peers clientes. Mesmo com a inexistência de peers provedores que cumprem as métricas de QoS publicadas, pode ocorrer do fornecimento de algum serviço, quando na requisição de serviço o peer cliente estabelecer um critério bem relaxado de métrica de QoS.

A inserção de apenas um peer provedor confiável (isto é, que cumpre o valor das métricas de QoS publicadas), a quantidade de violações de métricas de QoS cai para aproximadamente 32,4% quando no uso do SATYA e para 86,1% sem o uso. Este resultado reflete o uso dos valores de reputação no processo de descoberta de serviços, uma vez que peers não confiáveis tendem a não serem selecionados na maior parte do tempo pelos peers clientes. Entretanto, a presença de somente um peer provedor confiável no conjunto de peers provedores pode gerar um conjunto muito grande de requisição de serviços para este peer confiável, de forma que em um curto período de tempo este não possuirá mais recursos para fornecer o serviço dentro das métricas de QoS publicadas, a não ser que este peer provedor publique novos valores de métricas de QoS refletindo o seu estado atual. A adição de novos peers provedores confiáveis gera uma queda linear na porcentagem de violações de métricas de QoS publicadas com e sem o uso do SATYA.

5.4 Considerações Finais do Capítulo

Neste capitulo foram apresentada as simulações realizadas para o sistema de reputação proposto no Capítulo 3 para o cenário de uma Rede Metropolitana Sem Fio e a extensão deste sistema proposto no Capítulo 4 para um cenário de Serviços Web. As simulações foram feitas utilizando o simulador de redes *Network Simulator* com o módulo que realiza o cálculo de

sistemas nebulosos criados utilizando o editor visual da *Fuzzy Toolbox* do Matlab, implementado na linguagem C.

As simulações realizadas referentes ao Mecanismo de Cálculo de Reputação mostraram que a sua utilização minimiza o problema da ocorrência de formação de peers em conluio com o intuito de diminuir a reputação de um peer. A utilização deste mecanismo em um cenário baseado em Serviços Web que utiliza uma Arquitetura Orientada a Serviços, ao mesmo tempo em que forneceu medidas quanto à confiabilidade de provedores, também permitiu a validação das avaliações fornecidas pelos clientes, diminuindo o grau de subjetividade de tais avaliações e tornado-as uma métrica efetiva. Os grupos de preferência formados podem atuar como mecanismos de incentivo que aumentem a participação dos usuários no processo de distribuição de avaliações das métricas de QoS publicadas. Portanto, a abordagem proposta aumenta a confiança mútua entre clientes e provedores, alavancando o potencial de utilização da Web para transações comerciais.

Capítulo 6 Conclusão e Trabalhos Futuros

Este trabalho apresentou uma abordagem que utiliza um sistema de reputação como forma de aumentar a confiabilidade em nível de serviço em redes com múltiplos usuários capazes de interagir diretamente, sem a necessidade de uma infra-estrutura centralizada. O sistema de reputação proposto foi desenvolvido de forma modular e foi avaliado através da realização de simulações. Inicialmente, foi avaliada a aplicação do sistema em um cenário de Redes Metropolitanas Sem Fio com topologia Malha. Em seguida, o sistema de reputação foi estendido com a adição de novos módulos com o objetivo de aumentar a confiança no uso dos serviços em um cenário de baseado em Serviços Web que utiliza uma Arquitetura Orientada a Serviços.

De forma a abstrair a infra-estrutura do cenário utilizado foi utilizada uma rede Peer-to-Peer (P2P) sobreposta à infra-estrutura física da rede, criando uma topologia lógica de comunicação sobre a infra-estrutura do cenário de aplicação utilizado. A rede P2P apresenta uma arquitetura estruturada baseada no trabalho [40], utilizando um algoritmo de *Tabela Hash Distribuída.* Baseada nesta rede P2P os peers clientes e provedores trocavam serviços entre si, sem a distinção entre um peer ser exclusivamente um peer cliente ou um peer provedor.

Sendo assim, as características inovadoras presentes no sistema de reputação proposto são: (i) a utilização de um sistema de reputação, como os comumente adotados em redes P2P, para tratar do controle do acesso aos serviços oferecidos na rede; (ii) a adoção de uma abordagem orientada a serviços, que permite atribuir níveis de confiabilidade não somente a peers isoladamente, mas ao par *peer-serviço* utilizado; e (iii) o uso de lógica nebulosa para o cálculo das reputações atribuídas aos pares *peer-serviço* e os mecanismos utilizados para minimizar o problema do conluio.

A adoção de um sistema baseado em reputações trouxe o benefício de fornecer uma solução escalável, enquanto que a atribuição da reputação não somente ao peer, mas ao par *peer-serviço*, permitiu que um peer possa optar por fornecer ou não um serviço específico a um determinado peer, baseado em sua reputação. Com isso, a abordagem orientada a serviços do sistema de reputação proposto agregou um nível extra de segurança para as interações realizadas entre os peers, podendo ser utilizado em conjunto com outros mecanismos de segurança, como os mecanismos de criptografia, por exemplo.

Já o uso de Lógica Nebulosa no cálculo da reputação permitiu expressar e manipular valores imprecisos e subjetivos através do desenvolvimento de um sistema nebuloso. Foram

calculados dois valores de reputação denominados de Reputação Individual e Reputação Agregada. A Reputação Agregada, por apresentar a característica de utilizar todos os valores de avaliação do peer, possui a possibilidade de ocorrência do problema do conluio. Para minimizar o problema do conluio foram utilizados dois mecanismos: uma distribuição de freqüências e um filtro de atualização da reputação. A distribuição de freqüências tem o objetivo de descartar valores de avaliação fornecidos por peers feitas sem critério. Uma vez constatada que a nova avaliação pertence a distribuição de freqüências previamente calculada, o valor desta avaliação é submetido ao filtro de atualização para atualizar o valor de Reputação Agregada.

Complementando o trabalho, o sistema de reputação proposto foi estendido com novos módulos e aplicado a um cenário que utiliza Arquitetura Orientada a Serviços baseada em Serviços Web. A extensão do sistema de reputação, que foi denominado de SATYA, teve os objetivos de aumentar a confiança no processo de descoberta e seleção de serviços através do uso dos valores de reputação, sem um aumento significativo na sobrecarga de monitoramento da infra-estrutura de rede. Para realizar estes objetivos, o SATYA utilizou valores objetivos obtidos por entidades de monitoramento, denominadas Monitores de Desempenho, e avaliações fornecidas pelos clientes dos serviços.

De forma a calcular a reputação dos provedores, o SATYA utilizou o mesmo Mecanismo de Cálculo de Reputação (MCR) utilizado para o cenário de redes metropolitanas sem fio e apresentado no Capítulo 3. A principal diferença na utilização do MCR no SATYA está no cálculo da Reputação Individual dos peers provedores. Em vez de utilizar os peers pertencentes à Rede de Relacionamento do peer que requisita a reputação, foram utilizadas as avaliações fornecidas pelos peers pertencentes ao mesmo grupo de preferência do peer que requisitou a reputação. A utilização dos peers do mesmo grupo de preferência tem o objetivo de obter valores de reputação de peers que realizam avaliações considerando as mesmas métricas de QoS. Ao utilizar os valores do grupo de preferência para o cálculo da Reputação Individual pode acontecer o problema do conluio por serem utilizadas avaliações fornecidas por peers com os quais nunca interagiu. De forma a contornar este problema, o SATYA compara as avaliações subjetivas com os valores objetivos obtido pelo Monitor de Desempenho e efetua o descarte de avaliações com alto grau de discrepância. A Reputação Agregada, calculada utilizando todas as avaliações fornecidas pelos peers da rede, pode ser então utilizada por peers novos que ainda não pertençam a nenhum grupo de preferência, de forma a verificarem a reputação de um peer provedor quanto a confiabilidade em fornecer um

serviço de acordo com as métricas de QoS publicadas. Já o valor de Reputação Individual é utilizado para verificar o nível de confiabilidade em o provedor fornecer o serviço na métrica do grupo do peer cliente da requisição do serviço.

Sendo assim, os mecanismos apresentados no SATYA tiveram o objetivo de (i) diminuir o nível de subjetividade das avaliações fornecidas pelos clientes; (ii) prover valores de reputação que denotam a confiabilidade do provedor em fornecer o serviço de acordo com as métricas de QoS publicadas; (iii) criação de grupos de preferência de clientes que fornecem avaliações similares quanto ao uso dos serviços em uma determinada métrica de QoS e também, foram criados grupos de preferência de provedores de forma a agrupar provedores que fornecem um “melhor serviço” em uma determinada métrica de QoS. Além disso, os grupos de confiança criados podem então ser utilizados como mecanismo de incentivo para clientes fornecerem avaliações dos serviços.

Concluindo, o Sistema de Reputação proposto aumentou a confiabilidade das transações realizadas, beneficiando tanto provedores como clientes quanto a escolha confiável do par com o qual se deseja interagir.

6.1 Trabalhos Futuros

Quanto aos trabalhos futuros, pretende-se avaliar a suscetibilidade do sistema proposto a outros tipos de ataques além do conluio. Por exemplo, pretende-se avaliar o uso do Módulo de Cálculo de Reputação de forma a evitar o problema do ataque conhecido como nó traidor. A medida comumente utilizada na literatura [25] para evitar este tipo de ataque é a utilização do valor histórico de utilização dos serviços. O Módulo de Cálculo de Reputação pode ser então incrementado com os valores históricos e pode-se então avaliar o uso contra este tipo de ataque.

Um segundo trabalho futuro pode ser o desenvolvimento de uma aplicação baseada em serviços Web e que utilize os mecanismos para o cálculo da reputação e os módulos do SATYA, além de usar uma infra-estrutura P2P. Através do uso desta aplicação poderiam ser obtidas medidas quanto aos tempos de resposta para a obtenção dos valores de Reputação Individual e Agregada, entre outras. Uma outra direção de trabalho futuro relaciona o uso das avaliações subjetivas quando fornecidas para a avaliação de uma transação composta por vários Serviços Web. A investigação neste caso seria utilizar a avaliação subjetiva fornecida como uma única avaliação para todos os serviços individuais que compõem o Serviço Web, ou tratar cada serviço separadamente.

Por fim, como outro potencial trabalho futuro poderia ser verificada a utilização dos valores de reputação dos clientes por parte dos provedores como forma de otimizar os recursos de infra-estrutura de rede em um ambiente de comércio eletrônico baseado em Serviços Web. Neste ambiente, os provedores, baseados na reputação dos clientes, poderiam realizar uma seleção dos “melhores clientes” quanto à relação custo/benefício dos recursos utilizados do provedor e usar essa informação para diferentes finalidades. A relação custo/benefício pode ser, por exemplo, a quantidade de tráfego gerado pelo cliente em relação ao gasto financeiro feito por este. E um exemplo de uso dessa informação seria um provedor que, ao realizar uma campanha de *marketing* de venda de um produto utilizando o correio eletrônico, ao invés de enviar uma mensagem para todos os clientes cadastrados na sua base de clientes em certo instante, poderia enviar inicialmente mensagens para os clientes que possuem uma reputação alta. Em seguida, seriam enviadas mensagens para os clientes com reputação média, e assim por diante. Ao enviar as mensagens primeiro para os clientes que possuem uma reputação alta, o provedor espera que o retorno financeiro destes seja maior, e como foi limitado o número de mensagens enviadas, a sobrecarga da infra-estrutura do provedor quando os clientes abrirem a mensagem e enviarem requisições para o provedor será menor. Com isso, o cliente também ficará satisfeito com a possibilidade de ter uma baixa latência no provedor ao utilizá-lo. Após um período de tempo, podem então ser enviadas mensagens para os clientes que possuem uma reputação média, e assim sucessivamente.

REFERÊNCIAS BIBLIOGRÁFICAS

1. LAGES, A. G., DELICATO, F. C., PIRMEZ, L., *Um Sistema de Reputação Fuzzy para Segurança Orientada a Serviços em Redes de Banda Larga sem Fio*. Em XXIV Simpósio Brasileiro de Redes de Computadores (SBRC 2006), Curitiba, PR – Brasil, 2006.

2. LAGES, A. G., DELICATO, F. C., PIRMEZ, L., *Sistema de Reputação Orientado a Serviços baseado em Lógica Nebulosa*. Em VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG 2006), Santos, SP – Brasil, 2006.

3. LAGES, A. G., VIANNA, G. K., DELICATO, F. C., PIRMEZ, L. *A Service-Oriented Fuzzy Reputation System to Increase the Security of a Broadband Wireless Metropolitan Network*. Em 14th IEEE International Conference on Networks, 2006.

4. PIRES, P. F., DELICATO, F. C., LAGES, A. G., PIRMEZ, L., *SAS: Sistema de Avaliação de SLAs para Comércio Eletrônico baseado em Serviços Web*. Em XXV Simpósio Brasileiro de Redes de Computadores (SBRC 2007), Belém, PA – Brasil, 2007.

5. PIRES, P. F., DELICATO, F. C., LAGES, A. G., PIRMEZ, L., *SATYA: A Reputation-based Approach for Service Discovery and Selection in Service Oriented Architectures*. Em 9th ACM International Workshop on Web Information and Data Management, Lisboa, Portugal, 2007.

6. RESNICK, P., ZECKHAUSER, R., FRIEDMAN, E., KUWABARA, K., *Reputation Systems*. Em: Communications of the ACM, Vol. 43, Dezembro, 2000.

7. SONG, S., HWANG, k., KWOK, Y. and ZHOU, R., *Trusted P2P Transactions with Fuzzy Reputation Aggregation*. Em: Security in P2P Systems, IEEE Internet Computing, Novembro-Dezembro, 2005.

8. KAMVAR, S., SCHLOSSE, M. and GARCIA-MOLINA, H., *The EigenTrust Algorithm for Reputation Management in P2P Networks*. Em: Proceedings of the Twelfth International World Wide Web Conference, Maio, 2003.

9. DESPOTOVIC, Z. and ABERER, K., *P2P Reputation Management: Probabilistic Estimation vs. Social Networks*. Em: Journal of Computer Networks, Special issue on Management in Peer-to-Peer Systems: Trust, Reputation and Security, Elsevier, 2005.

10. Sítio Mercado Livre, http://www.mercadolivre.com.br, Último acesso: Agosto de 2007.

11. Sítio Ebay, http://www.ebay.com, Último acesso: Agosto de 2007.

12. BUCHEGGER, S., BOUDEC, J.Y.L., *A robust reputation system for p2p and mobile ad-hoc networks*. Em: Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, 2004.

13. JOSANG, A., ISMAIL, R., *The Beta Reputation System*. Em: Proceedings of the 15th Bled Eletronic Commerce Conference, 2002.

14. WITHBY, A., JOSANG, A. INDULSKA, J., *Filtering out Unfair Ratings in Bayesian Reputation Systems*. Em: Proceedings of the 7th International Workshop on Cooperative Information Agents, 2000.

15. W3C Working Draft [Online]. *Web services description language* (WSDL) Version 2.0 Part 1: Core Language. Em: http://www.w3.org/TR/. Último Acesso: Dezembro de 2007.

16. CLEMENT, L., HATELY, A., RIEGEN, C., ROGERS, T., *UDDI V. 3.0 Specification* [Online]. Em: http://www.uddi.org/pubs/uddi_v3.htm. Último acesso: dezembro 2007.

17. MAJITHIA, S., SHAIKH, A., RANA, O., WALKER, D., *Reputation-based Semantic Service Discovery*. Em: Proceedings of the 13th IEEE WET ICE, 2004.

18. WISHART, R., ROBINSON, R., INDULSKA, J., JSANG, A., *SuperstringRep: Reputation-enhanced Service Discovery*. Em: Proceedings of the 28th Australasian Computer Science Conference, Australia, 2005.

19. KELLER, A., LUDWIG, H., *The WSLA Framework Specifying and Monitoring Service Level Agreements for Web Services*. Journal Of Network And Systems Management, 11(1), pp. 57-81, Kluwer Academic Publishers, 2003.

20. Sítio Amazon, http://www.amazon.com, Último acesso: Agosto de 2007.

21. SINGH, M. P., HUHNS, M. N. *Service-Oriented Computing: Semantics, Processes, Agents*, Wiley, 2005.

22. MCKNIGHT, D. H., CHERVANY, N. L., *The meanings of Trust*. Technical Report MISRC Working Paper Series, 96-04, 1996.

23. JOSANG, A., ISMAIL, R., BOYD, C. *A Survey of Trust and Reputation Systems for Online Service Provision*. Em: Decision Support Systems, 43(2), pages 618-644, 2007.

24. THEOTOKIS, S. A., SPINELLIS, D., *A Survey of Peer-to-Peer File Sharing Technologies*. White paper, Electronic Trading Research Unit (ELTRUN), Athens University, 2002.

25. FELDMAN, M., LAI, K., STOICA, I., CHUANG, J., *Robust Incentives Techniques for Peer-to-Peer Networks*. Em: Proceedings of the 5th ACM conference on Eletronic Commerce, pages 102-111, 2004.

26. FELDMAN, M., PAPADIMITRIOU, C., STOICA, I., CHUANG, J., *Free-Riding and Whitewashing in Peer-to-Peer Systems*. Em: Proceedings SIGCOMM workshop on Practice and Theory of Incentives and Game Theory in Networked Systems, 2004.

27. ABDUL-RAHMAN, A., HAILES, S., Supporting Trust in Virtual Communities. Em: Proceedings of the Hawaii International Conference on System Sciences, 2000.

28. CRUZ, A., *Lógica Nebulosa*. Disponível em http://equipe.nce.ufrj.br/adriano/fuzzy/. Último acesso: Agosto de 2007.

29. BARCELLOS, M. P. ; GASPARY, L. P., *Segurança em Redes P2P: Princípios, Tecnologias e Desafios*. Em: XXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, p. 211-260, 2006.

30. ROCHA, J. B., DOMINGUES, M., CALLADO, A., SOUTO, E., SILVESTRE, G., KAMIENSKI, C., SADOK, D., *Peer-to-Peer: Computação Colaborativa na Internet*. Em: XXII Simpósio Brasileiro de Redes de Computadores, v. 1, p. 3-43, 2004.

31. Simple Object Access Protocol – SOAP, http://www.w3.org/TR/soap12, Versão 1.2.

32. ZADEH, L., *Fuzzy Sets*. Em: Information and Control, vol. 8, 338–353, 1965.

33. SINGH, A. and LIU, L., *TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems*. Em: Proceedings 3rd International Conference Peer-to-Peer Computing (P2P 2003), IEEE CS Press, pp. 142–149, 2003.

34. KALEPU, S., KRISHNASWAMY, S., LOKE, S.W. *Verity: A QoS Metric for Selecting Web Services and Providers*. Em: Proceedings of WISEW, pp: 131- 139, 2003.

35. LIU, Y., NGU, A.H., ZENG, L.Z., *QoS Computation and Policing in Dynamic Web Service Selection*. Em: Proceedings of the 13th WWW conference, pp: 66 -73, 2004.

36. JURCA, R., FALTINGS. B. *Reputation-based Pricing of P2P Services*. Em: Proceedings of ACM SIGCOMM'05 Workshops, Philadelphia, USA, pp: 144-149, 2005.

37. DELLAROCAS, C., *Goodwill Hunting: An Economically Eficient Online Feedback*. Em: Proceedings of the Workshop on Agent-Mediated Electronic Commerce, pages 238-252, 2002.

38. KALEPU, S., KRISHNASWAMY, S., LOKE, S.W. *Reputation = f(user ranking, compliance, verity).* Em: Proceedings of the IEEE ICWS, pp. 200- 207, 2004.

39. SHERCHAN, W., LOKE, S. W., and KRISHNASWAMY, S. *A fuzzy model for reasoning about reputation in web services*. Em: Proceedings of the 2006 ACM SAC, pp. 1886-1892, 2006.

40. TRIANTAFILLOU, P., *Peer-to-Peer Network Architectures: The Next Step*. Em: SIGCOMM Workshop on Future Directions in Network Architectures (FDNA-03), Agosto, 2003.

41. SHAMIR, A., *Identity-based cryptosystems and signature schemes*. Em: Advances in Cryptology: Proceedings of CRYPTO, 1984. p. 47–53.

42. BONEH, D., FRANKLIN, M. K., *Identity-based encryption from the weil pairing*. Em: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. London, UK, 2001. p. 213–229.

43. STOICAY, I., MORRIS, R., LIBEN-NOWELL, D., KARGER, D.R., KAASHOEK, M. F., DABEK, F., BALAKRISHNAN, H., *Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications*. Em: IEEE/ACM Transactions on Networking, ACM Press, vol. 11, no. 1, pp. 17–32, 2003.

44. ROWSTRON, A., DRUSCHEL, P., *Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems*. Em: IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Heidelberg, Germany, pages 329-350, November, 2001.

45. ZHAO, B., HUANG, L., STRIBLING, J., RHEA, S. C., JOSEPH, A. D., KUBIATOWICZ, J. D., *Tapestry: A Resilient Global-Scale Overlay for Service Deployment*. Em: IEEE Journal on Selected Areas in Communications, Vol 22, No. 1, January, 2004.

46. MatLab, http://www.mathworks.com/, Último acesso: Agosto de 2007.

47. Sítio Bondfaro, http://www.bondfaro.com.br, Último acesso: Agosto de 2007.

48. Sítio Buscapé, http://www.buscape.com.br/, Último acesso: Agosto de 2007.

49. ADOMAVICIUS, G.; TUZHILIN, A., *Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions*. Em: IEEE Transactions on Knowledge and Data Engineering, Volume 17, Issue 6, Page(s):734 – 749, Junho, 2005.

50. WEI, K., HUANG, J., FU, S., *A Survey of E-Commerce Recommender Systems*. Em: International Conference on Service Systems and Service Management, Page(s):1 – 5, Junho, 2007.

51. WANG, W., ZHAO, L., YUAN, R., *Improving cooperation in peer-to-peer systems using social networks.* Em: Proceedings of the 20th IPDPS, Rhodes Island, Greece, 2006.

52. NS2, http://www.isi.edu/nsnam/ns/, Último acesso: Dezembro de 2006.

53. ZIMMERMANN, P. R. 1995 *The Official PGP User's Guide*. MIT Press.

Apêndices

Apêndice A

Este apêndice contém as regras utilizadas pelo MCT para o cálculo sem tendência a uma métrica de QoS.

Tabela 7 – Regras utilizadas pelo MCT para o cálculo sem tendência

Regra	Regra Difusa
01	**If** (Conformidade-TR is CMB) **or** (Conformidade-DS is CMB) **or** (Conformidade-DE is CMB) **then** (Sem-Tendência is TMB)
02	**If** (Conformidade-TR is CMB) **or** (Conformidade-DS is CMB) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TMB)
03	**If** (Conformidade-TR is CMB) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CMB) **then** (Sem-Tendência is TMB)
04	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CMB) **or** (Conformidade-DE is CMB) **then** (Sem-Tendência is TMB)
05	**If** (Conformidade-TR is CMB) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TBX)
06	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CMB) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TBX)
07	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CMB) **then** (Sem-Tendência is TBX)
08	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TBX)
09	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TBX)
10	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TBX)
11	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TBX)
12	**If** (Conformidade-TR is CBX) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TME)
13	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CBX) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TME)
14	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TME)
15	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CBX) **then** (Sem-Tendência is TAL)
16	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TAL)
17	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TAL)
18	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CON) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TAL)
19	**If** (Conformidade-TR is CON) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TAL)
20	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CON) **or** (Conformidade-DE

	is CAL) **then** (Sem-Tendência is TAL)
21	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CON) **then** (Sem-Tendência is TAL)
22	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TMA)
23	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CMA) **then** (Sem-Tendência is TMA)
24	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CMA) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TMA)
25	**If** (Conformidade-TR is CMA) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TMA)
26	**If** (Conformidade-TR is CAL) **or** (Conformidade-DS is CMA) **or** (Conformidade-DE is CMA) **then** (Sem-Tendência is TMA)
27	**If** (Conformidade-TR is CMA) **or** (Conformidade-DS is CAL) **or** (Conformidade-DE is CMA) **then** (Sem-Tendência is TMA)
28	**If** (Conformidade-TR is CMA) **or** (Conformidade-DS is CMA) **or** (Conformidade-DE is CAL) **then** (Sem-Tendência is TMA)
29	**If** (Conformidade-TR is CMA) **or** (Conformidade-DS is CMA) **or** (Conformidade-DE is CMA) **then** (Sem-Tendência is TMA)