Sistema de Reputação Orientado a Serviços baseado em Lógica Nebulosa

Alexandre Gomes Lages[1], Flávia C. Delicato[2], Luci Pirmez[1]

[1]Universidade Federal do Rio de Janeiro – Núcleo de Computação Eletrônica
Prédio do CCMN - Bloco C, Caixa Postal: 2324 - CEP: 20.010-974
Cidade Universitária - Ilha do Fundão, Rio de Janeiro, RJ
[2]Universidade Federal do Rio Grande do Norte – Departamento de Informática e Matemática Aplicada
Campus Universitário Lagoa Nova, 59072-970, Natal, RN
{alexandrelages, luci}@nce.ufrj.br, flavia.delicato@dimap.ufrn.br

Abstract. *In the current Web environment users are able to directly interact to exchange data and services, without intermediation of central authorities. Such scenarios raise the need of efficient systems to assure the safety and confidence of transactions. Reputation Systems, which are widely used in P2P networks, have the goal of individually evaluating peers, relying on their previous interactions in the network. Reputation Systems could be used to increase the security on a service level. We propose the use of a service-oriented reputation system based on fuzzy logic as a solution to increase the security on a service level. This paper presents the description of the proposed system and the simulations carried out to evaluate it.*

Resumo. *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 redes P2P, têm como objetivo a avaliação individual de peers, baseando-se nas suas interações prévias. Tais sistemas podem ser utilizados para garantir a segurança em nível de serviços. Este artigo propõe o uso de um Sistema de Reputação orientado a serviços e baseado em lógica nebulosa, como forma de aumentar o nível de segurança dos serviços trocados entre estações. O artigo apresenta a descrição do sistema proposto, o cenário de aplicação e as simulações realizadas para sua avaliação.*

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 variada 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 existência de mecanismos que garantam a segurança e a confiabilidade dos pares envolvidos nas comunicações.

A utilização de arquiteturas de segurança centralizadas para a realização desta tarefa pode tornar a escalabilidade da rede limitada, além do fato de representar um ponto de falha único no sistema, diminuindo sua robustez. A utilização de uma arquitetura de comunicação distribuída que permita que estações realizem, por exemplo, transações eletrônicas de compra e venda de produtos, poderá contribuir para o aumento do tamanho da rede. Adicionalmente, além de mecanismos para aumentar a segurança nas informações trocadas entre as estações (em nível de enlace e de estação), são também necessários mecanismos para o aumento da segurança ao nível de utilização de serviços pelas estações. Com esse intuito, abordagens distribuídas para prover segurança em nível de serviço, como a utilização do mecanismo de

Chaves Públicas, ou a utilização de modelos baseados em Sistemas de Reputação, podem ser utilizadas.

Os modelos baseados em Sistemas de Reputação [1] são bastante utilizados em redes *Peer-to-Peer* (P2P) e se baseiam em interações prévias ocorridas entre os *peers*. Após um *peer* utilizar um serviço de outro, é atribuído ao *peer* um conceito referente à sua utilização deste serviço. De acordo com as interações passadas e com os conceitos que um *peer* possui, pode ser gerado um indicador sobre possíveis ações que um *peer* pode realizar no futuro. Um *peer* pode ter um valor de reputação para com diversos outros *peers*, com o qual interagiu, e a partir destes valores pode ser realizado o cálculo para a obtenção de um valor único, determinando a reputação global deste *peer*. Podem ser utilizados métodos estatísticos, como a média ou média ponderada, ou Lógica Nebulosa (*Fuzzy Logic*) [5] para a realização deste cálculo. A adoção de Lógica Nebulosa permite que se considerem valores imprecisos ou subjetivos na atribuição da reputação de uma estação, sendo esta uma característica desejável por assemelhar-se mais a forma como seres humanos realizam seus julgamentos.

O uso de modelos de reputação para garantir a segurança do *peer* em redes P2P é uma alternativa preferível à utilização de mecanismo de Chaves Públicas o qual, por necessitar de uma estrutura centralizada, possui escalabilidade limitada. Abordagens distribuídas, como as baseadas em Sistemas de Reputação, apresentam-se como uma solução mais robusta e escalável. 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. Outro problema que afeta os Sistemas de Reputação é a natureza dinâmica com que os *peers* entram e saem da rede, de forma que os valores armazenados por esses podem ser perdidos, caso não exista uma infra-estrutura para manter um nível de redundância no armazenamento das reputações sobre os *peers*.

Além dos ambientes P2P, outro cenário onde um Sistema de Reputação pode ser aplicado para o aumento da segurança dos serviços disponíveis é em uma Rede Sem Fio com topologia Malha (*Mesh*). Nessas redes, uma Estação-Assinante pode trocar informações com outras estações, entrar e sair da rede, sem necessidade de comunicação com uma Estação-Base. 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.

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 [2, 3, 4], o valor de reputação é atribuído ao próprio *peer*, e é usado para nortear suas interações com os outros *peers*. Nenhum trabalho, até o momento, apresenta um sistema de reputação cuja abordagem seja orientada a serviço, ou seja, onde a reputação atribuída refere-se ao par ***peer-serviço*** utilizado, e não ao *peer* isoladamente.

Neste trabalho propõe-se a utilização de um Sistema de Reputação com uma abordagem orientada a serviço. Adotou-se como cenário de aplicação do sistema proposto uma Rede Metropolitana Sem Fio com topologia Malha, pois tais redes precisam ter um sistema eficiente de segurança para auxiliar os usuários a localizarem parceiros confiáveis e trocarem serviços de maneira segura. 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 cômputo da reputação do mesmo; (iii) o processo para evitar a formação de conluios; e (iv) os resultados das simulações realizadas com o protótipo.

Quanto as contribuições do trabalho, destaca-se em primeiro lugar a proposta do mecanismo para a realização do cálculo da reputação atribuída ao par *peer-serviço*. Em um ambiente de serviços existirão comunidades específicas que utilizam um determinado serviço, como por exemplo, comunidade de usuários de Vídeo-Conferência e comunidade de Voz sobre IP, e um *peer* pode pertencer a uma ou várias destas comunidades. Para o cálculo da reputação

atribuída ao par *peer-serviço* são utilizados os valores de reputação dos *peers* não somente dentro de uma comunidade (processo denominado de **Reputação Local**), mas os valores obtidos de todas as comunidades a que este pertence (**Reputação Agregada**).

Outra contribuição importante é a forma de atualização da reputação de um *peer*. A fim de evitar o processo de conluio, um *peer*, ao receber um valor de reputação, deve verificar se tal valor está dentro de um padrão de distribuição de graus de reputação atribuída ao par *peer-serviço* em questão. Caso este valor esteja fora do padrão, o mesmo é descartado, sendo, entretanto utilizado no cálculo de futuras reputações do *peer*. Caso o valor esteja dentro do padrão de distribuição dos valores de reputação referentes ao par *peer-serviço*, o processo de atualização é realizado, efetuando-se o incremento ou decremento da reputação, baseado no grau de relacionamento e na reputação atribuída ao par *peer-serviço* que atribuiu o novo valor de reputação.

Este artigo está organizado nas seguintes seções: a Seção 2 descreve os trabalhos relacionados na área e a Seção 3 detalha o modelo de segurança distribuído proposto para um cenário de uma Rede Metropolitana de Banda Larga Sem fio com topologia Malha. Na Seção 4 é apresentada a forma como é calculado o grau de reputação do par *peer-serviço*, através da utilização de Lógica Nebulosa. Na Seção 5 são apresentados os testes realizados com o intuito de avaliar o mecanismo proposto. Por fim, a Seção 6 apresenta as considerações finais.

2. Trabalhos Relacionados

O sítio Mercado Livre [9] utiliza um processo de cálculo de reputação denominado **Processo de Qualificação**, que avalia os usuários após a compra ou venda de produtos no sítio. É utilizado um processo centralizado para o armazenamento das qualificações dos usuários e as informações 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 o valor de reputação. Outra desvantagem 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 uma qualificação mais refinada.

Em [10] é apresentando um Sistema de Reputação que utiliza uma arquitetura distribuída para armazenar valores sobre a reputação dos *peers*, com a característica de manter anônimos os *peers* responsáveis pelo armazenamento, dessa forma 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. Quando um *peer* deseja conhecer a reputação de outro é utilizado o processo de inundação na rede, apresentando como desvantagem um grande consumo de banda.

Em [3] é apresentado 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 o protocolo *Chord* [6]. De posse das reputações é realizada uma média ponderada dos valores para o cálculo final da reputação.

O trabalho descrito em [2] é o que apresenta maior semelhança com a presente proposta. Nele é proposto um algoritmo que utiliza Lógica Nebulosa para o cálculo da reputação global de um *peer*. Entretanto, tal trabalho não adota a abordagem orientada a serviços, sendo os valores de reputações atribuídos aos *peers* isoladamente. Além disso, no artigo não é tratado a possibilidade de um *peer* ter acesso a um serviço, mesmo tendo ele uma baixa reputação.

Em ambos os trabalhos [2, 3] não é tratada a possibilidade de formação de conluios dentro da rede P2P. Como estes trabalhos utilizam um algoritmo global de reputação, um grupo de *peers* pode ser formado com o intuito de aumentar ou diminuir o grau de reputação de um ou vários *peers*. Para evitar que este problema afete as reputações armazenadas nos *peers*

pertencentes à rede, no presente trabalho são utilizados dois filtros no momento em que o *peer* recebe um valor de reputação para armazenar em sua tabela. A reputação de um *peer* será atualizada somente se o valor de reputação passar pelos dois filtros com sucesso.

Com o intuito de minimizar o problema da formação de conluios, em [4] é empregado um dos dois métodos para o cálculo da reputação: (i) utilização dos valores de reputação de um determinado *peer* presentes em todos os *peers*, para a realização de um cálculo mais eficiente da sua reputação, ou (ii) utilização de métodos estatísticos em somente uma parte da rede. Para o cálculo da reputação usando o primeiro método é utilizado um multigrafo representando as interações entres os *peers*. Percorrendo as arestas deste grafo podem ser gerados os valores representativos do grau de reputação de um *peer*. 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 da rede de relacionamento.

3. Modelo de Segurança Orientado a Serviços

Um dos objetivos desse trabalho é propor um sistema de segurança baseado em reputação orientada a serviço. Para tal, adotou-se um cenário de uma rede metropolitana (MAN) sem fio com topologia Malha. O sistema proposto tem um papel importante no provimento de segurança de serviços nessas redes, no sentido em que oferece suporte para a troca confiável de serviços diretamente entre as estações-assinantes.

A segurança de acesso disponível nas redes metropolitanas sem fio baseia-se na utilização da subcamada de segurança definida no padrão IEEE 802.16, denominada *Privacy Sublayer*, que provê mecanismos de autenticação e criptografia das mensagens em nível de enlace. Entretanto, para explorar toda a potencialidade e flexibilidade disponibilizada por uma rede com topologia Malha é importante a utilização de mecanismos de segurança em nível de serviços, para que assinantes legítimos possam, de forma segura, trocar informações ou serviços diretamente entre eles. Sistemas de Reputação [1] são uma das abordagens para prover segurança em nível de serviço.

Quanto aos serviços tratados pelo Sistema de Reputação proposto, eles serão os mesmos definidos pelo padrão IEEE 802.16 das redes sem fio metropolitanas. Nessas redes foram definidas quatro classes de serviços, a saber: (i) serviço de concessão não solicitada (*Unsolicited Grant Service* - UGS); (ii) serviço para aplicações em tempo real (*Real-Time Polling Service* - rtPS); (iii) serviço para aplicações que não necessitam de tempo real (*Non-Real-Time Polling Service* - nrtPS); e (iv) serviço para aplicações de encaminhamento de tráfego através do melhor esforço (*Best Effort Service* - BE). Cada estação da rede (*peer*) pode estar associada a uma ou mais classes de serviços. Um *peer* associado a uma dada classe de serviço pode apresentar um comportamento diferente quando associado a uma outra classe de serviço. Conseqüentemente, esse *peer* possuirá valores de reputação diferentes para cada classe de serviço ao qual está associado.

3.1. Funcionalidades do Sistema de Reputação Orientado a Serviço

Em geral, os Sistemas de Reputação fazem uso das experiências prévias dos *peers* para atribuir níveis de reputação a recursos ou a outros *peers*. Tais sistemas assumem que os *peers* mantêm o mesmo identificador durante todo o período de tempo em que estiverem dentro do sistema. Em diversos trabalhos [2, 3, 4], o valor da reputação é atribuído pelo usuário, após uma interação com um *peer*.

No Sistema de Reputação com abordagem orientada a serviço proposto, o cálculo do valor da reputação é função do uso de um serviço por um *peer*. As informações sobre as interações com outros assinantes são armazenadas nos *peers* em uma base de reputação local, denominada **Tabela Grau de Reputação de Serviço**. Esta tabela possui quatro campos: um

campo para identificar a classe de serviço (IDS); um campo para identificar o *peer* (IDP); um campo contendo o grau de **Reputação** desse *peer* em relação a essa classe de serviço; um campo representado o grau de **Relacionamento** do *peer* que está armazenando a tabela em relação a esse *peer*.

O campo IDS tem como função identificar a classe de serviço usada pelo *peer*, que no cenário adotado serão as mesmas classes do padrão IEEE 802.16 conforme já mencionado (*UGS, rtPS, nrtPS,*ou *BE*). Cada classe de serviço pode atender aos requisitos de QoS de diversas aplicações. Por exemplo, a classe de serviço de melhor esforço pode atender as aplicações de transferência de arquivos e e-mail.

Um *peer*, ao receber um valor de reputação atribuído a um dado par *peer*-serviço para armazenar, utilizará os campos IDP e IDS para identificar o *peer* e o serviço associados ao valor de reputação a ser armazenado. Cada *peer* possui como identificador uma chave pública, que é única ao longo das entradas e saídas do *peer* da rede. A opção pelo uso de chave pública como identificador de um *peer* foi motivada pela necessidade de manter a integridade das informações armazenadas pelo mesmo. O modelo de distribuição de chaves adotado foi o SPKI/SDSI, proposto por [11, 12], o qual possui uma abordagem descentralizada para o processo de autenticação das chaves.

Os campos Reputação e Relacionamento são variáveis que representam experiências passadas de interação entre os *peers* com o serviço em questão e armazenam valores no intervalo [0,1]. Toda vez que um *peer* utiliza um serviço, o campo Reputação é atualizado com base nas ações executadas por este. O processo de busca e armazenamento do campo Reputação de um dado *peer* será explicado na Seção 3.3.

Ao longo do tempo, o *peer* hospedeiro do serviço atualiza o campo Relacionamento da Tabela Grau de Reputação de Serviço de forma a indicar o seu nível de interação em relação a cada *peer*. Quanto mais próximo de um estiver o valor do campo Relacionamento, maior terá sido a interação do serviço em questão com o *peer* e mais confiável será o valor correspondente armazenado no campo Reputação. O valor deste campo pode tanto ser incrementado quanto decrementado, dependendo das interações realizadas entre os *peers*.

Quando um *peer* deseja solicitar pela primeira vez o uso de um serviço de outro *peer*, duas situações podem ocorrer: o *peer* possui um convite ou não. Na primeira situação, o *peer* utiliza o convite, que é uma mensagem contendo o IDP e IDS associados, enviado por um outro *peer* já usuário desse serviço, que então herda a reputação do *peer* que emitiu o convite. Na segunda situação, o *peer* não possui um convite. Neste caso, o *peer* que hospeda o serviço deve tomar a decisão de fornecê-lo ou não para o novo *peer* e, em seguida, calcular a sua reputação. A possibilidade de um *peer* ter permissão para utilizar um serviço, mesmo ser ter um convite, faz com que novos *peers* possam entrar na rede sem nenhum valor de reputação associado. Entretanto, o *peer* hospedeiro do serviço deverá utilizar-se de políticas específicas para o fornecimento ou não dos seus serviços. Uma possível política consiste no *peer* hospedeiro consultar os *peers* pertencentes a sua rede de relacionamentos e ver se algum deles possui informações sobre o par *peer*-serviço em suas tabelas. A partir dessas informações o hospedeiro toma a decisão de prover ou não o serviço. Tal decisão é função de características específicas e do nível de segurança requerido pelo serviço. O comportamento do *peer* solicitante é avaliado após a utilização do serviço e o resultado é refletido na atualização do campo Reputação da Tabela Grau de Reputação de Serviço do *peer* hospedeiro.

3.2. Reputação Agregada de um Peer

Em geral, uma classe de serviço engloba diversas aplicações. Ao se utilizar uma aplicação, a reputação de um *peer* estará associada inicialmente à instância particular daquela aplicação. Os valores de reputação por instância de aplicação são armazenados em uma tabela auxiliar. Como uma classe de serviços engloba diversas aplicações, um valor único é calculado por classe e tal

valor é armazenado na Tabela Grau de Reputação de Serviço. Os pesos das reputações do *peer* em relação a cada aplicação de uma mesma classe são iguais. Para fins de simplicidade, durante a descrição do presente trabalho assume-se que cada classe de serviços engloba apenas uma aplicação. Para o cálculo da reputação agregada, são utilizadas as reputações do *peer* em cada classe de serviço, aonde cada classe de serviço possui diferentes pesos (prioridades).

3.3. Descrição do Mecanismo de Busca de Reputação

Uma rede P2P com arquitetura estruturada [6, 7, 8] foi escolhida por realizar de forma rápida a busca e a inserção dos valores de reputação calculados, já que requer um menor número de mensagens para a obtenção da reputação de uma estação. Entretanto, as redes estruturadas possuem a desvantagem de utilizar uma topologia definida, geralmente em Anel, de forma que o custo de manutenção dos *peers* na rede torna-se elevado com o aumento de tamanho da mesma. Para contornar este problema, será utilizada uma rede denominada **Rede Sobreposta de Reputação** (RSR), executando o protocolo Chord [6] adotado, com a única função de armazenar a reputação dos peers da rede. A Figura 2 apresenta a estrutura da rede utilizada.

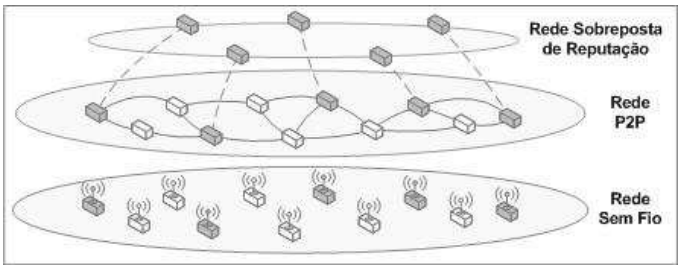

Figura 1. Rede Sobreposta de Reputação

As estações pertencentes à RSR terão como função o armazenamento da reputação e devem possuir a característica de permanecerem grandes períodos de tempo conectado na 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 RSR de maneira dinâmica, de modo a não comprometer a escalabilidade da rede na qual o sistema esteja sendo utilizado. A relação da quantidade de estações pertencentes a rede RSR e a rede na qual está sendo utilizado o sistema de reputação é deixada como trabalho futuro.

Para a recuperação da reputação de um peer utilizando o protocolo Chord, o *peer* hospedeiro do serviço aplica uma função de *hash* para a descoberta da chave que identifica o *peer* responsável pelo armazenamento da reputação do *peer* que solicitou o serviço. Duas ou mais funções de *hash* podem ser utilizadas, aumentando a redundância da informação. A Figura 2 mostra o *peer* S solicitando um serviço ao *peer* A, sendo tal solicitação representada pela linha contínua. Ao receber a solicitação, o *peer* A executa dois algoritmos de *hash* para a obtenção de duas chaves distintas, e em seguida, envia requisições para estes *peers* sobre a reputação do *peer* S. As linhas tracejadas, partindo do *peer* A para os *peers* B e N representam esta interação.

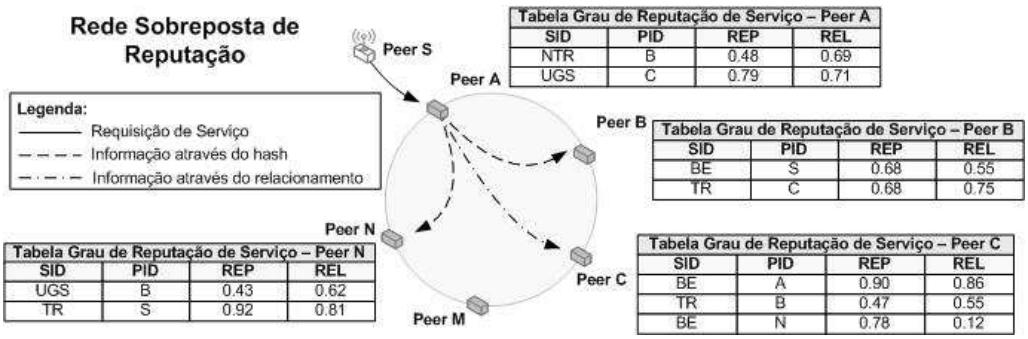

Figura 2. Módulo de Comunicação e Cálculo da Reputação

Um diferencial da presente proposta consiste na adoção de uma etapa adicional de obtenção de informação, além das executadas no protocolo *Chord*, com o intuito de aumentar a confiabilidade da informação de reputação. Nessa etapa adicional, são enviadas, a partir do *peer* hospedeiro (no exemplo o *peer* A), solicitações para *peers* considerados como "Amigos" (*peer* C), isto é, *peers* que possuam um alto valor no campo Relacionamento. Essas solicitações são enviadas com o intuito de obter informações com maior chance de acerto sobre a reputação (1) do *peer* solicitante do serviço (*peer* S); e (2) dos *peers* responsáveis pelo armazenamento da reputação do *peer* solicitante (*peers* B e N). Considerando a Figura 2, C retornará a reputação do S, caso ele a possua, e também as reputações dos *peers* B e N, responsáveis pelo armazenamento da reputação de S. O envio de solicitações pelo *peer* hospedeiro não somente para os *peers* retornados pelo algoritmo *hash*, mas também para os *peers* considerados "Amigos" é justificado, pois os *peers* "Amigos" podem possuir um valor mais confiável da reputação do *peer* solicitante do que os outros retornados pelo algoritmo *hash*. Assim, as informações de reputação retornadas por esses "Amigos" terão um peso maior no cálculo da reputação. Adicionalmente, esses *peers* "Amigos" podem também informar o valor da reputação dos *peers* retornados pelo algoritmo de *hash*, caso o *peer* hospedeiro do serviço não a possua. Caso não seja possível obter os valores sobre a reputação dos *peers* retornados pelo algoritmo de *hash* e dos *peers* "Amigos", os *peers* retornados pelo algoritmo de *hash* terão um valor baixo, próximo de zero, para o campo Relacionamento, de forma que a influência do valor de reputação retornado por estes *peers* seja considerada muito baixa no cálculo da reputação final do peer solicitante do serviço.

4. Cálculo da Reputação utilizando Lógica Nebulosa

Nesta seção são apresentados dois processos de inferência utilizados para o cálculo da reputação de um *peer*, um para realizar o cômputo da reputação de um *peer* e outro para evitar que, com a formação de conluio na rede, a reputação de um *peer* possa ser alterada.

4.1. Processo de Avaliação da Reputação Local de um *Peer*

O procedimento responsável pelo cálculo da reputação de um par *peer-serviço* baseia-se em Lógica Nebulosa e é denominado de **Cálculo de Reputação Nebuloso**. No presente trabalho, o "Cálculo de Reputação Nebuloso" foi implementado no ambiente *Matlab*, utilizando-se o *FIS Editor*. A primeira etapa na execução do Cálculo compreende a definição das variáveis nebulosas, bem como dos conjuntos nebulosos referentes a cada uma das variáveis nebulosas consideradas. Após a realização de uma fase de análise, foram identificadas duas variáveis de entrada e uma de saída, a serem usadas pela máquina de inferência para o cálculo da reputação de um par *peer*–serviço. Tais variáveis estão descritas a seguir.

Grau-Reputação (variável de entrada): contém o grau de reputação de um par *peer*–serviço retornado por um *peer* que forneceu o serviço ***(Muito alto, Alto, Médio, Baixo, Muito Baixo)***.

Grau-Relacionamento (variável de entrada): contém o grau de relacionamento entre o *peer* que enviou a reputação e o *peer* responsável por armazená-la para um dado serviço ***(Amigo, Colega, Desconhecido)***.

Reputação-Final (variável de saída): resultado do Cálculo de Reputação Nebuloso que representa o valor da reputação final que deve ser armazenado em função do relacionamento entre os peers para um dado serviço (o peer que enviou e o peer responsável pelo armazenamento) ***(Muito alto, Alto, Médio, Baixo, Muito Baixo)***.

A forma gráfica dos conjuntos nebulosos (triângulo, sigmóide, trapézio, etc.) representa a função de pertinência do conjunto, sendo o seu rótulo o indicativo da semântica a este associada. No presente trabalho, a construção da semântica dos conjuntos nebulosos foi efetuada, como já mencionado, a partir dos resultados obtidos pelas simulações realizadas.

Após a conclusão da etapa de definição de todas as variáveis nebulosas, com seus conjuntos e regras semânticas, foram construídas as regras de inferência, as quais complementam a construção do sistema nebuloso. A combinação de todas as variáveis nebulosas de entrada, resultantes do processo de *nebulização*, pode gerar até 15 regras possíveis na base de regras difusas. A superfície (a) da Figura 4 sintetiza graficamente as regras usadas e apresenta o valor retornado da reputação em função dos valores de reputação e relacionamento do mesmo.

Finalizando o processo, a máquina de regras difusas determina quais regras serão ativadas pelos valores de entrada (variáveis nebulosas citadas) a fim de determinar quais conjuntos nebulosos de saída sofrerão o processo de *desnebulização*. A saída do Cálculo de Reputação Nebuloso referente a variável nebulosa de saída reputação-final pode ser Muito Alto, Alto, Médio, Baixo, Muito Baixo. O processo de *desnebulização* é o responsável por determinar o resultado escalar de saída e, no procedimento proposto, consiste em determinar o grau de reputação de um *peer*.

Como a reputação de um *peer* está armazenada em diversos *peers*, para o cálculo da reputação final é realizada uma média dos valores retornados pelo procedimento "Cálculo de Reputação Nebuloso" (dos *peers* retornados pelo algoritmo de *hash* e dos *peers* amigos).

Por exemplo, na Figura 22 o *peer* S solicita um serviço do *peer* A. O *peer* A, ao executar o algoritmo de *hash*, retorna os *peers* N e B como responsáveis pelo armazenamento da reputação de S. Os valores da reputação de S retornados por N e B são 0.92 (Muito Alto) e 0.68 (Alto), respectivamente. O *peer* A conhece somente a reputação do *peer* B, e o seu grau de relacionamento com este é de 0.69 (Amigo). O *peer* C retorna a informação de que o *peer* N está em sua tabela e tem como valor de reputação 0.78 e de relacionamento o valor 0.12 (Desconhecido). As informações de reputação e de relacionamento de B armazenadas em C também são enviadas para o *peer* A (0.47 e 0.55, respectivamente). Em seguida, é usada a máquina de inferência para calcular a reputação do *peer* A em relação a B ($Fuzzy_{a,b}$) e a N ($Fuzzy_{a,n}$). Quanto ao cálculo da reputação de A em relação a B, o procedimento Cálculo de Reputação Nebuloso recebe como variável de entrada escalar os respectivos valores: 0.68 e 0.69, para reputação e relacionamento, respectivamente. O processo de *desnebulização* mapeia o conjunto nebuloso ALTA da variável nebulosa de saída reputação no escalar 0.59.

Quanto ao cálculo da reputação de A em relação a N, o procedimento "Cálculo de Reputação Nebuloso" recebe como variável de entrada escalar os respectivos valores, 0.92 e 0.12, para as variáveis reputação e relacionamento. O processo de *desnebulização* mapeia o conjunto nebuloso **MÉDIA** da variável nebulosa de saída reputação no escalar 0.56. De posse destes valores, o *peer* A tem como calcular a reputação de S calculando a média dos valores obtidos. Assim, a reputação final do *peer* S será: S = (0.59 + 0.56) / 2 = 0.575.

4.2. Processo de Avaliação da Reputação Agregada de um Peer

Para realizar o cálculo da reputação ***Agregada*** de um *peer*, todos os valores de reputação que o *peer* possui em todas as classes de serviço são agregados e um valor único de reputação é gerado. Como citado na seção 4.2, as classes de serviço possuem prioridades diferentes. No cenário apresentado, por exemplo, a classe de serviço UGS possui prioridade mais alta, enquanto a classe de serviço BE possui prioridade mais baixa dentre as quatro. Assim, um *peer* que possui uma reputação alta na classe BE e um valor baixo na classe UGS pode ter como resultado uma valor baixo de reputação ***Agregada***. Para realizar o cálculo da reputação ***Agregada*** do *peer*, utiliza-se uma média ponderada dos valores das reputações nas classes de serviço que o *peer* já utilizou. Por motivos de restrição de espaço, a discussão quanto ao momento do disparo do processo de avaliação de um *peer* após a utilização de um Serviço está fora do escopo desse trabalho.

4.3. Atualização da Tabela Grau de Reputação de Serviço

Cada *peer* é responsável por manter a Tabela Grau de Reputação de Serviço contendo os valores de reputação e relacionamento de outros *peers* e estes valores serão atualizados de acordo com a freqüência com que os *peers* utilizam os serviços existentes na rede. Um *peer* pode receber valores de reputação de diversos *peers* existentes na rede. Para evitar que a tabela seja alterada por *peers* que estão em processo de formação de conluio na rede, antes do armazenamento dos valores na tabela, os mesmos são primeiramente avaliados quanto à natureza da distribuição de todos os valores de reputação recebidos e, em seguida, aplica-se uma equação para o cálculo e armazenamento final da reputação na tabela.

4.3.1. Filtro na Distribuição dos Valores de Reputação

Como visto, um *peer* possui um conjunto de valores de reputação, um para cada classe de serviço que ele utilizou. Além dessas reputações, um *peer* também mantém uma base de valores históricos de reputação por serviço e por *peer*, recebidos de um determinado *peer*. De posse dessa base de valores históricos, um *peer* poderá aceitar ou rejeitar o valor de reputação recebido de outros *peers*, para efeitos de atualização da sua tabela.

Quando um *peer* recebe um novo valor para armazenar, primeiramente é verificado se o valor de reputação recebido está dentro de um padrão de distribuição. Tal verificação tem o propósito de evitar que um *peer* que possua um determinado histórico de valores de reputação seja penalizado por um *peer* que informa um valor baixo de reputação para o mesmo, fora da sua média e desvio padrão. Neste trabalho, os valores históricos de reputação são modelados utilizando uma distribuição normal. Valores de reputação recebidos que estejam um certo valor porcentual fora da distribuição no momento da recepção são descartados para fins de atualização da tabela. Entretanto, tais valores são inseridos na base de valores históricos de reputação por serviço e por *peer*, de forma que sucessivos valores de reputação fora do padrão possam alterar o padrão de distribuição. Assim, em um momento futuro, o *peer* poderá atualizar a tabela com valores que estariam fora do padrão de distribuição se este não fosse alterado.

4.3.2. Filtro para a Atualização da Tabela Grau de Reputação de Serviço

Após um *peer* receber de outro *peer* um valor de reputação para ser armazenado na Tabela Grau de Reputação de Serviço, e verificar que esse valor está conforme ao padrão de distribuição, tal valor não é imediatamente armazenado. Antes é executado um segundo processo com o intuito de evitar oscilações na atualização do grau de reputação e, conseqüentemente, diminuir a possibilidade de formação de conluios. Tal processo é dependente do valor de relacionamento entre o *peer* que está informando o grau de reputação e o *peer* que está armazenando esse valor. A fim de evitar oscilações na atualização dos graus de reputação de um *peer*, devem ser considerados os valores anteriores do grau que está sendo atualizado. Para isso, usa-se o filtro, descrito pela expressão da Figura 3.

$$\mathrm{Rep}_{\mathrm{peer}} = \alpha * \mathrm{Rep}_{\mathrm{media}} + (1 - \alpha) * \mathrm{Rep}_{\mathrm{nova}}$$

Figura 3. Fórmula para evitar oscilações na atualização do grau de reputação

Na fórmula da Figura 3 é atribuído a $\mathbf{Rep_{peer}}$ o resultado do cálculo do valor da reputação média do *peer* ($\mathbf{Rep_{média}}$) e da nova reputação ($\mathbf{Rep_{nova}}$). Um diferencial deste trabalho relaciona-se ao método proposto para obter o valor de α. Para o estabelecimento do valor da variável α, deve ser levado em conta o valor de relacionamento do *peer* que está enviando a mensagem contendo a reputação do *peer* com o *peer* responsável pelo armazenamento dessa reputação na Tabela Grau de Reputação de Serviço. Dessa maneira, quanto maior o grau de relacionamento, menor será o valor α (maior peso para $\mathrm{Rep}_{\mathrm{nova}}$), e vice-versa.

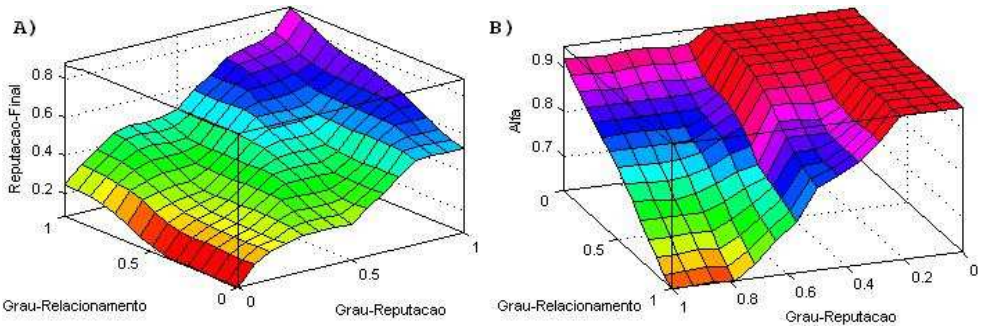

Figura 4. Superfície para o cálculo da Confiança (A) e Alfa (B)

Dessa maneira, caso os *peers* que estão enviando os valores de reputação possuam um baixo relacionamento com o *peer* responsável pelo armazenamento da reputação, o valor utilizado para α será alto e seu impacto na atualização da tabela será baixo. A superfície (b) da Figura 4 apresenta os valores de α que são gerados, a partir do valor de relacionamento e reputação recebidos de um *peer*. Esta superfície foi gerada através da criação de uma máquina de inferência nebulosa com variáveis de entrada **Grau-Reputação** (variáveis lingüísticas: Muito Alto, Alto, Médio, Baixo e Muito-Baixo) e **Grau-Relacionamento** (variáveis lingüísticas: Amigo, Colega e Desconhecido) e variável de saída **Alfa** (variáveis lingüísticas: Pequeno, Médio, Alto).

5. Avaliação do Sistema de Reputação Orientado a Serviço para o Cenário de uma Rede Metropolitana de Banda Larga sem Fio

Nesta seção são apresentados os testes realizados para testar o Sistema de Reputação proposto. No primeiro teste será verificada a variação da reputação de um peer que está sobre um ataque de conluio, e no segundo teste será apresentada a quantidade de serviços que foram acessados com sucesso por um peer sofrendo o mesmo ataque. Nas simulações utilizou-se o simulador de redes ns2 [13], e como cenário de aplicação os serviços definidos de uma Rede Metropolitana Sem Fio com topologia Malha. Foi simulada uma rede sem fio 802.11 com um total de 60 nós em uma área de 100x100. Cabe ressaltar que para a realização dessa etapa de testes não foi necessária a simulação do protocolo *Chord* ou de um ambiente de rede 802.16, visto que os testes foram realizados em nível de aplicação do sistema de reputação proposto.

5.1. Simulação da Variação da Reputação

A primeira etapa de testes tem como objetivo analisar o problema da formação de conluio. Ao receber um valor para armazenar na Tabela Grau de Reputação de Serviço, deve ser realizado um teste para verificar se tal valor está dentro do padrão de distribuição dos valores de reputação do peer. Caso não esteja dentro do padrão, este valor é descartado, sendo, entretanto, registrado na base de valores históricos de reputação por serviço, para fins de atualização dos valores usados no cálculo da distribuição. Caso esteja dentro do padrão de distribuição, o novo valor de reputação será atualizado conforme a expressão da Figura 3. Na avaliação da proposta, realizou-se a comparação do comportamento de atualização da reputação propostas de trabalhos anteriores [2, 3], os quais utilizam valores fixos para a variável α e não realizam o descarte antecipado.

Os gráficos da Figura 5 mostram a variação do grau de reputação que um peer A recebe para armazenar referente a um peer B. No teste foi utilizada somente uma função de hash para o armazenamento da reputação do peer B. Simulou-se a formação de conluio envolvendo 5%, 10%, 20%, 30%, 40% e 50% de peers na rede, com valor de reputação inicial do peer B de 0.5. Foram realizadas 30 rodadas em cada um dos grupos de conluio, sendo calculados em seguida a média, o desvio padrão e o intervalo de confiança de 95%. O tempo de simulação total de cada rodada foi de 3000 segundos, sendo que durante os primeiros 300 segundos de simulação, os

peers integrantes do grupo de conluio não afetam a reputação do peer B. Entretanto, passados os 300 segundos, tais integrantes começariam a afetar a reputação do peer B, retornando valores de reputação entre Muito Baixo e Baixo para o peer B, caso fossem acessados. Quando o peer acessado não integrar o grupo do conluio, é retornado o valor de reputação representando as ações realizadas pelo peer B, entre Muito Alta e Alta.

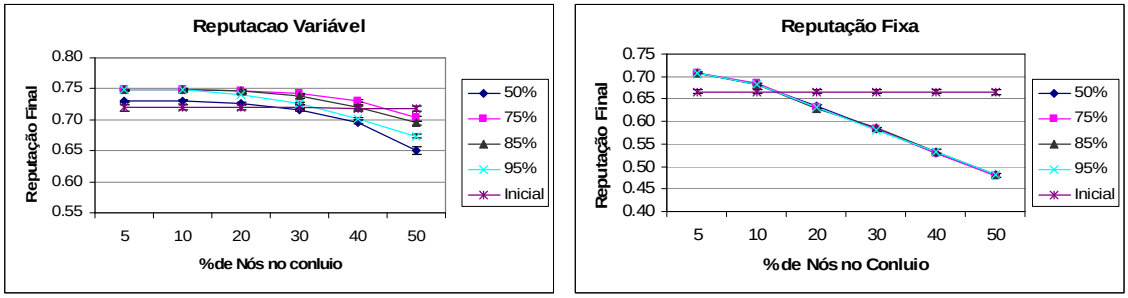

Figura 5. Atualização da Tabela Grau de Reputação de Serviço – (a) Nebuloso (b) Fixo

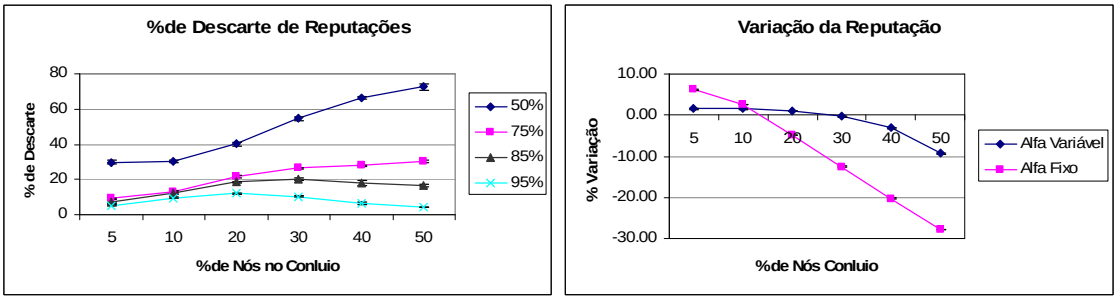

Figura 6. (a) Porcentagem de Descarte de Reputação (b) Variação do Grau de Reputação

O gráfico (a) da Figura 5 mostra as curvas referentes a reputação média final do peer B, usando a fórmula da Figura 3 (valor de α variável) e utilizando os valores de 50%, 75%, 85% e 95% como descarte na distribuição. É apresentada também uma curva com o valor médio inicial da reputação do peer B antes da formação do conluio (isto é, até o tempo de simulação de 300 segundos). Ao comparar as curvas, constata-se que até a formação de um conluio de aproximadamente 25% dos nós da rede, a reputação final do peer B não possui uma diferença negativa em relação a sua reputação inicial. A queda apresentada pela curva com parâmetro de 50% é mais acentuada que as demais devido à política mais conservadora no descarte das reputações recebidas. Com o aumento da porcentagem dos nós na formação do conluio, os valores de reputação recebidos pelo peer A para armazenar apresentam grandes diferenças, fazendo com que ocorra um maior número de descartes de reputações. O gráfico (a) da Figura 6 apresenta a porcentagem de notas descartadas para efeito da atualização da Tabela Grau de Reputação de Serviço. Conforme mostra o gráfico, a porcentagem de notas descartadas utilizando um parâmetro de 50% é aproximadamente de 73% quando na ocorrência de um grupo de conluio de 50% do total de peers na rede.

O gráfico (b) da Figura 5 mostra as curvas referentes à reputação média final do peer B, usando valores de comportamento apresentado em trabalhos anteriores [2, 3] (valor fixo de 95% para a variável α e sem descarte antecipado). As quatro curvas apresentam uma sobreposição devido à inexistência da política de descarte antecipado. Neste gráfico também é apresentada a reputação média inicial do peer B, resultante após 300 segundos de simulação. Ao comparar as quatro curvas representando a reputação final do peer B com a curva representando a reputação inicial, constata-se que o valor de reputação começa a apresentar uma diferença negativa em relação a reputação inicial a partir da formação de um grupo de conluio com tamanho de aproximadamente de 12%. A diferença entre a curva inicial e as curvas finais é bastante grande quando comparada com a utilização de um α variável e uma

política de descarte de reputações antecipado. O gráfico (b) da Figura 6 mostra a diferença entre as reputações iniciais e finais do peer B em relação a utilização da política de descarte antecipada e α variável contra a utilização do α fixo somente. A partir das curvas do gráfico (b) da Figura 6, com um grupo de conluio de tamanho de 30% da rede, a diferença entre as reputações inicial e final com descarte antecipado e α variável é próxima de zero, enquanto com a utilização do α fixo, a mesma diferença está em torno de 12,5% negativa. Para casos envolvendo um grupo de conluio de 50%, as duas curvas apresentam aproximadamente 9% e 28% negativo, com a utilização da política de descarte e α variado contra α fixo, respectivamente.

Comparando os dois métodos, ou seja, o que considera o valor de α variável e utiliza a política de descarte (proposto nesse trabalho) e o que considera α fixo, observa-se que, com o aumento do tamanho do grupo de conluio, o valor da reputação final do peer B para α fixo apresenta um comportamento linear na queda da reputação. A partir de um grupo de tamanho correspondendo a 11% de peers da rede, a utilização de um α fixo apresenta uma resultado inferior do que com o método proposto no presente trabalho. Já a curva com o α variável e com política de descarte, a curva apresenta uma queda mais suave, com uma reputação final negativa de 9% aproximadamente para um grupo de conluio representando 50% de peers. Tal fato deve-se a proposta apresentada nesse trabalho adotar descarte antecipado de valores e atualizar a tabela de reputação utilizando um α proporcional ao nível de relacionamento entre os peers. Em suma, a proposta de atualização da Tabela Grau de Reputação de Serviço usando o descarte e o filtro da Figura 3 é mais **resiliente** do que as propostas apresentadas nos trabalhos anteriores mencionados.

5.2. Simulação da Quantidade de Serviços Acessados com Sucesso

A Figura 7 apresenta dois gráficos representando a quantidade de serviços requisitados por um peer sofrendo um ataque de conluio e que foram realizados com sucesso. O gráfico (a) da Figura 7 mostra a quantidade de acessos aceitos para um serviço cuja reputação mínima é de 0.5 (Reputação Média), ou seja, somente é permitido ao peer acessar o serviço caso este tenha uma reputação mínima de 0.5, caso contrário, o acesso é negado. O gráfico (b) apresenta as mesmas informações para o caso de um serviço cuja reputação mínima é de 0.7 (Reputação Alta). Neste teste, somente são computados os acessos a serviços que não pertencem a peers que estão em conluio, uma vez que os peers em conluio sempre aceitam o serviço e retornam um baixo valor de reputação. Em ambos os testes são calculados o desvio padrão e o Intervalo de Confiança de 95% para 30 rodadas.

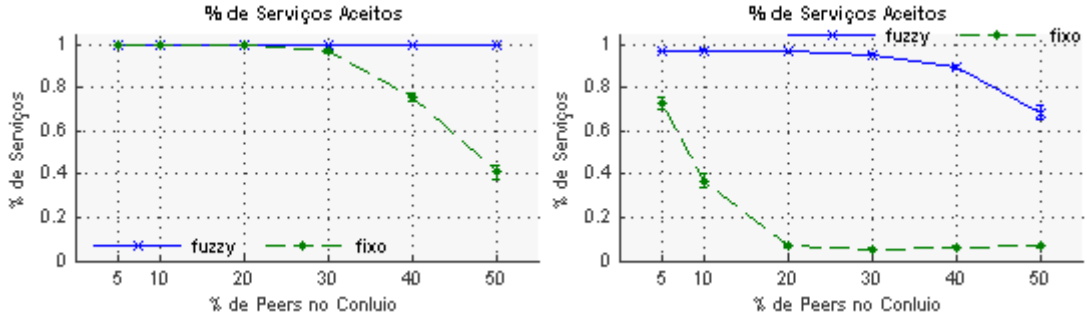

Figura 7. Porcentagem de serviços aceitos (a) Reputação Mínima 0.5 (b) Reputação Mínima 0.7

Conforme o gráfico (a) da Figura 7, para o caso de um peer honesto que esteja sofrendo um ataque de conluio, este peer conseguirá acessar todos os serviços que este requisitar, e no qual a reputação mínima do peer necessária seja de 0.5. Este resultado foi obtido por causa da utilização dos mecanismos propostos neste artigo (para cálculo e atualização da tabela de reputação). Entretanto, caso esteja utilizando propostas de outros trabalhos, com um grupo de

conluio de 30% do tamanho da rede, haverá em torno de 3% de acessos a serviços negados, e com um tamanho de 50% da rede, uma quantidade de 60% de acessos negados.

O gráfico (b) da Figura 7 apresenta a quantidade de acessos negados a um peer, cuja reputação mínima seja inferior a 0.7, Um peer sofrendo um ataque de conluio utilizando os mecanismos propostos terá uma queda na taxa de negação de acesso a serviços mais suave do que se utilizar propostas de trabalhos anteriores. Até um grupo de conluio de 30% do tamanho da rede, a taxa de sucesso é superior a 95%, enquanto para uma taxa de 20% do tamanho da rede, este peer terá em média 93% de acessos negados caso esteja utilizando propostas de trabalhos anteriores.

Também foram realizados testes para medir a taxa de acessos realizados com sucesso a serviços cuja reputação mínima do peer fosse 0.3, 0.4, 0.6 e 0.8. Para o caso de serviços que tenham como requisito uma reputação mínima do peer de 0.3 (Reputação Baixa), em ambos os casos (Fuzzy e Fixo) os acessos aos serviços podem ser realizados com 100% de sucesso. Este é um resultado necessário para que um peer não tenha problemas de não conseguir acessar nenhum serviço por este ter uma reputação baixa, e consequentemente, poder formar uma nova. A segurança dos acessos oferecidos para peers com reputação baixa por estes tipos de serviços não deve ser levada em consideração, uma vez que estes não envolvem serviços com alta segurança.

Para um serviço cuja reputação mínima do peer seja de 0.4, os testes apresentaram uma pequena taxa de negação de 2% para o caso de utilizar o parâmetro α Fixo, enquanto que utilizando o parâmetro α variável, todos os acessos foram obtidos com sucesso. Para serviços cuja reputação mínima do peer fosse de 0.6, utilizando α variável, o pior caso apresenta 2% de acessos negados para um grupo de conluio de 50%, e 84% de acessos negados para o mesmo tamanho de grupo de conluio utilizando α fixo. Já para o caso de um serviço cuja reputação mínima do peer seja de 0.8, apenas 1% dos serviços serão acessados com sucesso utilizando o α Fuzzy e com um grupo de conluio de 5% do tamanho da rede, enquanto que para outras variações de tamanho do grupo de conluio e utilizando o α fixo ou variável, o acesso é negado. Isto acontece porque serviços deste tipo requerem que os peers sejam bastante confiáveis e de tratarem de serviços com extrema segurança.

6. Considerações Finais

Este trabalho propôs uma nova abordagem para aumentar a segurança em nível de serviço em redes com múltiplos usuários capazes de interagir diretamente, sem a necessidade de uma infra-estrutura centralizada. A solução proposta foi aplicada em um cenário de redes metropolitanas sem fio de banda larga. As características inovadoras da proposta são: (i) a utilização de um modelo 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 estações (*peers*) isoladas, mas ao par *peer*-serviço utilizado; e (iii) o uso de lógica nebulosa para o cálculo das reputações atribuídas aos pares *peer*-serviço. O mecanismo para a troca de mensagens contendo os valores de reputação referentes aos pares *peer*-serviço baseou-se em um protocolo conhecido, o qual, porém, foi incrementado com etapas adicionais, tirando proveito da existência de uma rede de relacionamento entre os *peers*. Dessa forma, informações armazenadas em *peers* pertencentes a mesma rede de relacionamento são compartilhadas e usadas, tanto para o cálculo dos valores de reputação quanto para obter a reputação de *peers* solicitantes de serviços não conhecidos diretamente pelo *peer* provedor dos serviços. Os valores de reputação referentes a cada par *peer*-serviço são alterados dinamicamente, de acordo com os resultados das interações entre os *peers*. A atualização de tais valores baseia-se em mecanismos que buscam evitar ou minimizar a formação de conluios na rede e, ao mesmo tempo, reduzir o grau de oscilação nos valores de reputação armazenados. Testes realizados em ambiente simulado comprovaram a eficácia dos mecanismos propostos.

7. Referências

[1] Resnick, P., et al. (2000) “Reputation Systems”. In: Communications of the ACM, Vol. 43, December.

[2] Song, S., et al. (2005) “Trusted P2P Transactions with Fuzzy Reputation Aggregation”. In: Security in P2P Systems, IEEE Internet Computing, November-December.

[3] Kamvar, S., Schlosse, M. and Garcia-Molina, H. (2003) “The EigenTrust Algorithm for Reputation Management in P2P Networks”. In Proceedings of the Twelfth International World Wide Web Conference, May.

[4] Despotovic, Z. and Aberer, K. (2005) “P2P Reputation Management: Probabilistic Estimation vs. Social Networks”. In: Journal of Computer Networks, Special issue on Management in Peer-to-Peer Systems: Trust, Reputation and Security, Elsevier.

[5] Zadeh, L. “Fuzzy Sets” (1965), Information and Control, vol. 8, 338–353.

[6] Stoicay, I., et al. (2003) “Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications”. In: IEEE/ACM Transactions on Networking, ACM Press, vol. 11, no. 1, pp. 17–32.

[7] Rowstron, A. and Druschel, P. (2001) "Pastry: Scalable, distributed object location and routing for large-scale *peer*-to-*peer* systems". In: IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Heidelberg, Germany, pages 329-350, November.

[8] Zhao, B., et al. (2004) “Tapestry: A Resilient Global-Scale Overlay for Service Deployment”. In: IEEE Journal on Selected Areas in Communications, Vol 22, No. 1, January.

[9] Mercado Livre (2005), http://www.mercadolivre.com.br, Dezembro.

[10] Singh, A. and Liu, L. (2003) “TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems”. In: Proc. 3rd Int’l Conf. Peer-to-Peer Computing (P2P 2003), IEEE CS Press, pp. 142–149.

[11] Ellison, C. M., et al.(1999). “SPKI Certificate Theory”. Internet Engineering Task Force RFC 2693.

[12] Rivest, R. L. and Lampson, B. (1996). “SDSI – A simple distributed security infrastructure”.Presented at CRYPTO’96 Rumpsession.

[13] Network Simulator (2005), http://www.isi.edu/nsnam/ns/, Dezembro.