

Avaliação de Métodos Matemáticos usados nos Modelos de Reputação de Incentivo à Cooperação *

Fabiana Martins da Silva¹, José Ferreira de Rezende¹

¹Grupo de Teleinformática e Automação - PEE - Coppe
Universidade Federal do Rio de Janeiro (UFRJ)

{fabiana, rezende}@gta.ufrj.br

Abstract. *The proposals of reputation mechanisms to incentive the cooperation, used in peer-to-peer networks to detect the presence of egoistic and malicious peers, are different mainly because the choice of mathematical method used in reputation calculation. Some proposals opt to simplicity, using methods as a simple average. Others consider the use of methods more complex as, for example, Bayes and the Dempster-Shafer Theory. Aspects of convergence, robustness and security of the methods must be well known because these aspects are extremely important when choosing the mathematical method to be implemented. This work do fair comparisons between them through the implementation of a simulator capable to test these different methods, placing them in equal conditions of tests and evaluating them with the same metrics and criterias.*

Resumo. *As propostas de mecanismos de incentivo à cooperação baseados em reputação, usados em redes peer-to-peer para detectar a presença de peers egoístas e maliciosos, se diferenciam principalmente na escolha do método matemático usado no cálculo da reputação. Algumas propostas optam pela simplicidade, usando métodos como uma média simples. Outras propõem o uso de métodos mais complexos como, por exemplo, Bayes e a teoria de Dempster-Shafer. Aspectos de convergência, robustez e segurança dos métodos devem ser bem conhecidos, pois são extremamente importantes no momento de decidir ou não pela implantação de um dado método. Este trabalho efetua comparações justas através da implementação de um simulador contemplando esses diferentes métodos, colocando-os em condições iguais de testes e avaliando-os segundo os mesmos critérios e métricas.*

1. Introdução

Sistemas *peer-to-peer* (P2P) vêm ganhando bastante importância e atenção nos últimos tempos. Já são encontradas diversas aplicações P2P que contam com um número cada vez maior de usuários. Segundo [Damiani et al. 2002], em setembro de 2002, já eram 100 milhões usuários do aplicativo para compartilhamento de arquivos KaZaA [KaZaA] e este número crescia numa taxa significativa de cerca de 3 milhões por semana.

Os sistemas P2P baseiam seu funcionamento em um importante fundamento: a cooperação entre os *peers* da rede, que desempenham tanto o papel de cliente, quanto o papel de servidor, compartilhando os mais variados tipos de recursos e

*Este trabalho recebeu recursos dos projetos Giga/RNP (Taquara e GigaBOT), CNPq, FAPERJ e FINEP.

serviços. Entretanto, estudos como [Saroiu et al. 2002], [Adar and Huberman 2000], [Asvanund et al. 2004] e [Hughes et al. 2005] demonstraram que boa parte dos usuários não obedece a esta premissa. Não é incomum a presença dos chamados usuários egoístas, que usam recursos de outros *peers* da rede e, no entanto, limitam ou impedem o acesso aos seus recursos. Também existem os *peers* maliciosos, que usam a rede apenas para prejudicar outros usuários como, por exemplo, disponibilizando arquivos infectados, corrompidos ou de conteúdo falso em uma rede de compartilhamento de arquivos.

A busca pela solução deste problema de mau comportamento levou ao desenvolvimento de diversas propostas de mecanismos de incentivo à cooperação. Uma das principais linhas de pesquisas explora o uso do conceito de reputação. A idéia é que cada *peer* tenha seu comportamento julgado pelos outros *peers* da rede com os quais interagiu e desenvolva, ao longo do tempo, uma reputação. Requisições feitas a *peers* com boa reputação têm maiores chances de serem bem sucedidas. Requisições recebidas de *peers* com má reputação não devem ser atendidas.

As propostas de incentivo à cooperação baseados em reputação podem ter duas arquiteturas: centralizada ou descentralizada. Na arquitetura centralizada, existe uma entidade central (*central authority*) responsável por calcular, manter e publicar a reputação de cada um dos nós que compõem a rede. Um famoso exemplo de aplicação desta arquitetura é o site eBay [eBay]. [Jøsang et al. 2005] descreve inúmeros outros exemplos.

Na arquitetura descentralizada, cada *peer* da rede mantém históricos de avaliações geradas a partir de suas experiências com outros *peers*. Uma avaliação é uma nota dada pelo *peer* que requisitou algum serviço/recurso, ao comportamento do *peer* que o atendeu. Estas informações são usualmente conhecidas por “informações de primeira mão”.

O cálculo da reputação pode ser baseado somente em informações de primeira mão, entretanto, em uma rede com muitos *peers* como, por exemplo, uma rede P2P de compartilhamento de arquivos, será comum a situação em que um *peer* deseja interagir com outro com quem nunca interagiu ou com quem teve poucas experiências, ou seja, de quem tem nenhuma ou pouca informação de primeira mão. Por causa disso, os *peers* trocam experiências entre si. As informações recebidas de outros *peers* são comumente chamadas de “informações de segunda mão”.

As propostas existentes baseadas em reputação de arquitetura descentralizada se diferenciam, principalmente, pela escolha do método matemático usado para o cálculo da reputação. Algumas propostas optam pela simplicidade, usando métodos como uma média simples enquanto outros trabalhos propõem o uso de métodos mais complexos como, por exemplo, Bayes e a teoria de Dempster-Shafer. A adoção de um mecanismo para contornar o problema de mau comportamento necessita de um bom entendimento das vantagens e desvantagens de cada método. Aspectos de convergência, robustez e segurança são extremamente importantes e devem ser bem conhecidos.

O objetivo deste trabalho é prover condições de efetuar comparações justas entre os métodos de cálculo de reputação, colocando-os em condições iguais de testes e avaliando-os segundo os mesmos critérios e métricas. Para atingir este objetivo foi criado um simulador, desenvolvido em C, que testará os métodos: *simpleAverage*, *exponentialAverage* [Yu et al. 2004], *DST* [Yu and Singh 2002a], [Yu and Singh 2002b], [Yu and Singh 2003], *enhancedReputation* [Liu and Issarny 2004] e *adaptedDST*.

2. Descrição dos Métodos Matemáticos

2.1. Média Simples

O uso de média simples é uma opção de baixa complexidade para calcular a reputação. Usando a proposta apresentada em [Yu et al. 2004], para que um *peer* P_i calcule a reputação de um outro *peer* P_j , o primeiro passo é a agregação das informações de primeira mão, feita pela função a seguir:

$$R(P_i, P_j) = \begin{cases} \sum_{k=1}^h e_{ij}^k / h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases}$$

onde e_{ij}^k é a k-ésima avaliação dada por P_i a P_j dentro do intervalo $[0, 1]$ e h é o número de avaliações presentes no histórico, que é capaz de armazenar H avaliações mais recentes. O valor considerado para H , usualmente, é 10.

A agregação das informações de segunda mão é dada por:

$$T(P_i, P_j) = \begin{cases} \sum_{k=1}^L w_k * R(W_k, P_j) / L & \text{if } L \neq 0; \\ 0.5 & \text{if } L = 0. \end{cases}$$

onde L é o número de testemunhas e w_k é a credibilidade que é dada a informação de segunda mão recebida da testemunha W_k . w_k pode assumir qualquer valor dentro do intervalo $[0, 1]$.

Nas simulações realizadas neste trabalho, considera-se que nenhum *peer* mente ao dar seu testemunho a respeito de outro e, portanto, w_k tem sempre o valor 1. Entretanto, mentir ao testemunhar é um ataque possível e fácil de ser praticado e, portanto, a maioria das propostas de mecanismos de incentivo à cooperação já inclui um mecanismo de credibilidade que torna os *peers* capazes de identificar se uma testemunha é mais ou menos honesta e associar a ela uma credibilidade. Versões futuras do simulador incluirão testes dos mecanismos de incentivo à cooperação em conjunto com os de credibilidade.

Por fim, a seguinte função é usada para o cálculo do valor final de reputação, agregando informações de primeira e segunda mão:

$$Rep(P_i, P_j) = \eta * R(P_i, P_j) + (1 - \eta) * T(P_i, P_j) \quad \text{onde, } \eta = h/H.$$

Portanto, quando o histórico de avaliações está cheio ($h=H$), a informação de segunda mão passa a não ser considerada no cálculo do valor final de reputação.

2.2. Métodos de Média Exponencial

Um dos possíveis ataques em redes P2P é a mudança repentina de comportamento. Um *peer* pode se comportar bem por um tempo com o intuito de desenvolver uma boa reputação perante os outros *peers* e depois passar a se comportar mal. Por causa deste ataque, alguns mecanismos de incentivo optam pelo uso de média exponencial. Dois destes mecanismos são estudados por este trabalho e serão descritos nas próximas seções.

Nos métodos exponenciais, o maior peso dado às avaliações mais recentes agiliza a convergência e, poucas interações falhas com um *peer* já causam uma redução suficiente em sua reputação para que seja considerado mal comportado. Entretanto, *peers* bem comportados não são infalíveis e também podem ter problemas para atender algumas requisições. Mecanismos com reação muito rápida podem entender algumas poucas falhas de um provedor bem comportado como uma mudança no seu comportamento.

2.2.1. Mecanismo exponentialAverage

A proposta de [Yu et al. 2004] usa a seguinte função para agregar informações de primeira mão:

$$R(P_i, P_j) = \begin{cases} (1 - \gamma)^{(h-1)} * e_{ij}^1 + (1 - \gamma)^{(h-2)} * \gamma * e_{ij}^2 + \dots + (1 - \gamma)^0 * \gamma * e_{ij}^h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases}$$

onde γ , variável chamada comumente de fator de decaimento ou mesmo pelo termo em inglês *fading factor*, pode assumir qualquer valor dentro do intervalo $[0, 1]$. Quanto mais próximo de 1 for o valor desta variável maior será o peso das informações mais recentes. e_{ij}^k representa a k-ésima avaliação dada por P_i a P_j dentro do intervalo $[0, 1]$ e h é o número de avaliações presentes no histórico, que é capaz de armazenar H avaliações mais recentes. O valor considerado para H , usualmente, é 10.

Este método usa as mesmas fórmulas descritas na Seção 2.1 para agregar as informações de segunda mão e para calcular o valor final da reputação.

2.2.2. Mecanismo enhancedReputation

Na proposta de [Liu and Issarny 2004] não há a utilização de históricos de avaliações. A cada interação entre dois *peers*, a seguinte função é usada:

$$R(P_i, P_j) = (1 - \gamma) * R(P_i, P_j)_{current} + \gamma * e_{ij}$$

onde γ , é o fator de decaimento ou *fading factor* (vide Seção 2.2.1). $R(P_i, P_j)_{current}$ representa o valor atual da informação de primeira mão que P_i possui de P_j e e_{ij} representa a avaliação mais recente. $R(P_i, P_j)_{current}$ e e_{ij} são valores dentro do intervalo $[-1, 1]$.

Para agregar as informações de segunda mão, a seguinte função é usada:

$$T(P_i, P_j) = \frac{\sum_{k=1}^L w_k * R(W_k, P_j)}{\sum_{k=1}^L w_k}$$

onde L é o número de testemunhas e w_k é a credibilidade (vide Seção 2.1) dada à informação de segunda mão recebida da testemunha W_k . w_k pode assumir qualquer valor dentro do intervalo $[0, 1]$.

Por fim, a seguinte função é usada para o cálculo do valor final de reputação, agregando informações de primeira e segunda mão:

$Rep(P_i, P_j) = \eta * R(P_i, P_j) + (1 - \eta) * T(P_i, P_j)$ onde, η é um valor dentro do intervalo $[0, 1]$ que define o peso da informação de primeira mão.

2.3. Métodos de Teoria de Dempster-Shafer

A teoria de Dempster-Shafer (DST: *Dempster-Shafer Theory*) é descrita em [Sentz 2002] como uma alternativa para a representação matemática da incerteza, que não pode ser feita através da teoria tradicional de probabilidade. Para introduzir os conceitos da DST, considera-se inicialmente que um *peer* P_i possui o conjunto $\theta = \{T, notT\}$ de hipóteses

(*frame of discernment*) a respeito do comportamento de um *peer* P_j , onde T representa a hipótese de P_j ser bem comportado, ou seja, confiável no fornecimento de algum serviço/recurso (*trust*), e notT representa a hipótese de P_j ser mal comportado, ou seja, não confiável no fornecimento de algum serviço/recurso.

A DST permite que P_i possua crenças $m(T)$ na hipótese de P_j ser confiável, $m(notT)$ na hipótese de P_j não ser confiável e $m(T, notT)$ representando incerteza. Os valores das crenças devem estar no intervalo $[0, 1]$ e seu somatório deve ser igual a 1. Não ter crença na hipótese do bom comportamento de um *peer* não quer dizer necessariamente acreditar no seu mau comportamento, como acontece na teoria tradicional da probabilidade. À medida que P_i passa a interagir e avaliar P_j , suas crenças são atualizadas e a incerteza vai dando lugar a maior crença em alguma das hipóteses de θ .

A DST também define uma regra de combinação que pode ser usada para agregar as crenças $m_r(T)$, $m_r(notT)$ e $m_r(T, notT)$ com as crenças $m_s(T)$, $m_s(notT)$ e $m_s(T, notT)$ originadas pelos *peers* P_r e P_s , respectivamente, a respeito do comportamento de um *peer* P_j :

$$m_{rs}(T) = \frac{m_r(T) * m_s(T) + m_r(T) * m_s(T, notT) + m_r(T, notT) * m_s(T)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))}$$

$$m_{rs}(notT) = \frac{m_r(notT) * m_s(notT) + m_r(notT) * m_s(T, notT) + m_r(T, notT) * m_s(notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))}$$

$$m_{rs}(T, notT) = \frac{m_r(T, notT) * m_s(T, notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))}$$

O estudo da DST como método de cálculo da reputação será feito através dos mecanismos descritos a seguir.

2.3.1. Mecanismo DST

A proposta dos artigos [Yu and Singh 2002a], [Yu and Singh 2002b] e [Yu and Singh 2003] assume que os clientes sempre avaliam os provedores com um dos 11 valores discretos $\{0.0; 0.1; 0.2; \dots 1.0\}$. Além disso, apresentam a função $f(x_k) = g/H$, onde x_k é um dos 11 valores discretos de avaliação, g é a quantidade de avaliações do histórico que assumem o valor x_k . O histórico é capaz de armazenar H avaliações mais recentes. O valor considerado para H, usualmente, é 10. Considere os limites inferior e superior ω e Ω , onde $0 \leq \omega \leq \Omega \leq 1$, as crenças $m(T)$, $m(notT)$ e $m(T, notT)$ relacionadas ao comportamento de um *peer* P_j podem ser calculadas por:

$$m(T) = \sum_{x_k=\Omega}^1 f(x_k) \quad m(notT) = \sum_0^{x_k=\omega} f(x_k) \quad m(T, notT) = \sum_{x_k=\omega}^{x_k=\Omega} f(x_k)$$

A regra de combinação de DST é usada para agregar as informações de segunda mão, ou seja, as crenças relacionadas ao comportamento de P_j que foram calculadas por outros *peers*. Neste mecanismo, a informação de primeira mão **não** é agregada à informação de segunda mão. Uma vez que o *peer* P_i possua seu histórico de avaliações de P_j cheio, ele considera apenas as crenças que ele próprio calcula usando as fórmulas mostradas acima. Enquanto seu histórico não está cheio, considera apenas as informações de segunda mão agregadas pela regra de combinação de DST.

2.3.2. Mecanismo adaptedDST

Este mecanismo é uma adaptação do mecanismo DST. Os cálculos são executados da mesma forma, exceto que a regra de combinação de Dempster-Shafer também é usada para agregar as crenças calculadas por P_i a partir de seu histórico de avaliações de P_j (informações de primeira mão) com as crenças resultantes da agregação das informações de segunda mão. Assim, a informação de segunda mão será sempre considerada no cálculo final da reputação.

3. O Uso da Reputação Calculada

Nos mecanismos `simpleAverage`, `exponentialAverage` e `enhancedReputation`, a reputação calculada para um *peer* é representada por um valor dentro de um intervalo ($[0, 1]$ para o `simpleAverage` e `exponentialAverage` e $[-1, 1]$ para o `enhancedReputation`). Este valor pode simplesmente ser comparado com valores limites no momento de concluir se este *peer* é ou não bem comportado. Se a reputação está abaixo de um limite inferior pré-definido, o provedor é considerado mal comportado e, se está acima de um limite superior, o provedor é considerado bem comportado.

Já no caso dos mecanismos que utilizam a DST, é preciso definir como as crenças calculadas serão usadas. O artigo [Yu and Singh 2003] apresenta uma maneira de converter as crenças em um valor único que expressa a probabilidade do *peer* de se comportar bem. Uma vez que essa conversão tenha sido feita, o julgamento de um *peer* pode ser feito da mesma maneira que nos demais mecanismos. A fórmula de conversão é:

$$prob(T) = \frac{m(T) + m(T, notT)}{1 + m(T, notT)}$$

4. O simulador

4.1. Parâmetros e Suposições da Geração do Cenário

Neste item, serão descritas as principais configurações feitas no simulador para a geração dos cenários usados nas simulações apresentadas neste documento.

O tempo de duração de cada simulação é configurado pela definição do número de interações entre clientes e provedores. As simulações mostradas neste trabalho são compostas de 80000 interações. O cenário considerado é constituído de 50 *peers*, 10 dos quais são unicamente provedores e 40 unicamente clientes. A quantidade de clientes que atuam como testemunhas em cada interação é 5. Numa rede P2P real, os *peers* exercem simultaneamente os papéis de cliente e servidor, entretanto, para simplificar a simulação e a interpretação dos resultados, foi assumido que os *peers* exercem somente um dos papéis.

Metade dos provedores tem bom comportamento enquanto que os outros são mal comportados. O comportamento de um dado provedor é a probabilidade deste provedor atender a uma requisição de um serviço/recurso feita por um cliente. Os provedores bem comportados estão configurados com o valor de 0.9 enquanto que os provedores mal comportados com 0.1. O número de provedores que mudam de comportamento no meio da simulação (ataque da mudança repentina de comportamento, vide Seção 2.2) é 1 em uma das simulações.

Está sendo considerado que todos os provedores oferecem um único serviço/recurso, que é do interesse de todos os clientes. Também é assumido que cada *peer* é capaz de identificar cada outro *peer* na rede e que, em caso de interesse, pode estabelecer com qualquer um deles uma comunicação direta.

4.2. Algoritmo de Geração do Cenário

O algoritmo de geração do cenário define, através de escolha aleatória, quais *peers* serão clientes, quais serão provedores, quais provedores serão bem e quais serão mal comportados e, ainda, quais terão comportamento variável. Nesta versão do simulador, são escolhidos aleatoriamente o cliente, o provedor e as testemunhas que irão participar de cada interação.

Durante a geração de cenário, os *peers* escolhidos para serem provedores, suas respectivas informações de comportamento e as informações relacionadas a cada interação (cliente, provedor e testemunhas escolhidos) são gravadas em arquivos possibilitando que o mesmo cenário possa ser usado em diversas simulações com diversos métodos matemáticos de cálculo da reputação.

4.3. Parâmetros e Suposições da Simulações

Neste item, serão descritas as principais configurações relacionadas às simulações dos métodos matemáticos nos cenários criados pelos parâmetros descritos na Seção 4.1.

Assume-se que um cliente cuja requisição foi atendida com sucesso fornece uma avaliação ao provedor maior ou igual a 0.6 para todos os mecanismos exceto para o `enhancedReputation` cujo valor deve ser 0.1 por conta do intervalo diferenciado de avaliação $[-1, 1]$. Um cliente cuja requisição não foi atendida ou foi atendida de maneira falha avalia o provedor com um valor menor ou igual a 0.4 para todos os mecanismos exceto para o `enhancedReputation` cujo valor considerado é -0.1.

Uma das justificativas para o uso do mecanismo DST é a possibilidade de manipular uma medida de incerteza. Em cenários onde as avaliações dadas por clientes a provedores fossem passíveis de falha e um cliente não conseguisse avaliar um provedor, este poderia associar a esta avaliação uma incerteza 1 e crenças em bom e mau comportamento 0. Os mecanismos que não fazem uso da DST teriam que recorrer a uma avaliação neutra, como por exemplo, 0.5 nos casos em que o intervalo de avaliação fosse $[0, 1]$. Para saber se alguma vantagem seria ganha com o uso da incerteza neste cenário, um dos parâmetros do simulador permite associar à avaliação uma probabilidade de falha.

O simulador é configurado para gerar um arquivo com o resultado de todas as interações e com as avaliações dadas pelos clientes de cada interação com os provedores. Desta forma, os diferentes métodos matemáticos de cálculo da reputação, ao ler este arquivo têm as mesmas informações, garantido assim, que os métodos são avaliados de maneira justa.

Uma reputação abaixo de 0.4 indica mau comportamento e uma acima de 0.6 bom comportamento. No método `enhancedReputation` estes valores são respectivamente -0.1 e 0.1. Uma reputação 0,5 é associada a um provedor novo ou desconhecido, para o qual não se calculou nenhum valor de reputação. No `enhancedReputation`, este valor é 0.

O fator de decaimento, usado pelos mecanismos `exponentialAverage` e `enhancedReputation` (vide Seções 2.2.1 e 2.2.2) é configurado como 0.5. O mecanismo `enhan-`

cedReputation tem ainda como parâmetro o peso da informação de primeira mão (vide Seção 2.2.2) cujo valor considerado é 0.6. Já o mecanismo DST tem dois parâmetros, os limites ω e Ω (vide Seção 2.3.1) cujos valores adotados são 0.4 e 0.6, respectivamente.

4.4. Algoritmo de Simulação

Em cada interação, o cliente requisita informações de segunda mão a respeito do provedor às testemunhas, agrega estas informações com as de primeira mão usando o método matemático configurado e verifica a reputação calculada para decidir requisitar ou não o serviço ao provedor. Se for requisitado, o provedor atende com sucesso ou não a requisição, dependendo do seu comportamento. Se for feita a requisição, o cliente avalia o provedor pela sua resposta, atualiza o histórico de avaliações associado a ele (se houver) e usa o método matemático escolhido para recalculá-lo seu valor de reputação.

4.5. Métricas

4.5.1. Percentual médio de decisões acertadas

Um *peer* toma uma decisão acertada quando decide não interagir com um provedor mal comportado ou interagir com um bem comportado. O percentual médio de decisões acertadas D é dado por:

$$D = \frac{\sum_{i=1}^C d_i / n_i}{C}$$

onde C é o número de clientes da rede que já fizeram alguma interação, d_i é a quantidade de decisões acertadas tomadas pelo cliente i e n_i é a quantidade total de interações feitas pelo cliente i .

4.5.2. Reputação Média

Para observar a evolução da reputação dos provedores em cada método, calcula-se a reputação média dos provedores bem comportados, dos mal comportados e dos provedores que aplicam o ataque da mudança repentina de comportamento. O cálculo é feito através da fórmula:

$$R = \frac{\sum_{i=1}^P \frac{\sum_{k=1}^C Rep(k,i)}{C}}{P}$$

onde C é o número de clientes da rede, $Rep(k, i)$ é a reputação que o cliente k calculou para o provedor i . Quanto a P , se a reputação média R que está sendo calculada é a dos provedores bem comportados, então P é o número de provedores bem comportados. Se R é a reputação média dos provedores mal comportados, então P é o número de provedores mal comportados. Se R é a reputação média dos provedores de comportamento variável, então P é o número de provedores de comportamento variável.

4.5.3. Percentual médio de provedores identificados

Como foi visto na Seção 4.3, se a um provedor está associada uma reputação abaixo de um limite inferior, ele é considerado mal comportado e, se a reputação do provedor está acima de um limite superior, ele é considerado bem comportado. Se um cliente calculou,

para um provedor bem comportado, uma reputação cujo valor é maior ou igual ao limite superior, diz-se que este cliente identificou que o provedor é bem comportado. Da mesma forma, se um cliente calculou, para um provedor mal comportado, uma reputação cujo valor é menor ou igual ao limite inferior, diz-se que este cliente identificou que o provedor é mal comportado. O Percentual médio de provedores bons identificados como bons é calculado por:

$$I = \frac{\sum_{i=1}^C p_i / P}{C}$$

onde C é a quantidade de clientes existentes na rede, p_i é a quantidades de provedores bons identificados pelo cliente i e P é a quantidade total de provedores bons presentes na rede.

Para o cálculo do percentual médio de maus provedores identificados como tais, a fórmula acima também é usada, entretanto p_i representaria a quantidades de provedores maus que foram identificados pelo cliente i e P seria a quantidade total de maus provedores presentes na rede.

4.6. Resultados dos Testes

Antes da discussão dos resultados, deve ser lembrado que a reputação calculada pelo método enhancedReputation está no intervalo $[-1, 1]$ e, para facilitar a análise do gráfico de reputações médias, os valores foram normalizados para o intervalo $[0, 1]$. No caso do método DST, as crenças são convertidas em um valor de probabilidade (vide Seção 3) e, nos gráficos de reputação média, é mostrada a média desta probabilidade. Os intervalos de confiança de cada gráfico foram omitidos para facilitar a visualização das curvas de tendência. Foram rodadas cinco simulações de cada cenário e os valores de variação máxima em torno da média, encontrados para cada método giram em torno de 5%, com exceção do gráfico da Figura 6, cujas curvas representam a reputação de um único provedor calculada por cada método. Neste caso a variação foi de cerca de 30% .

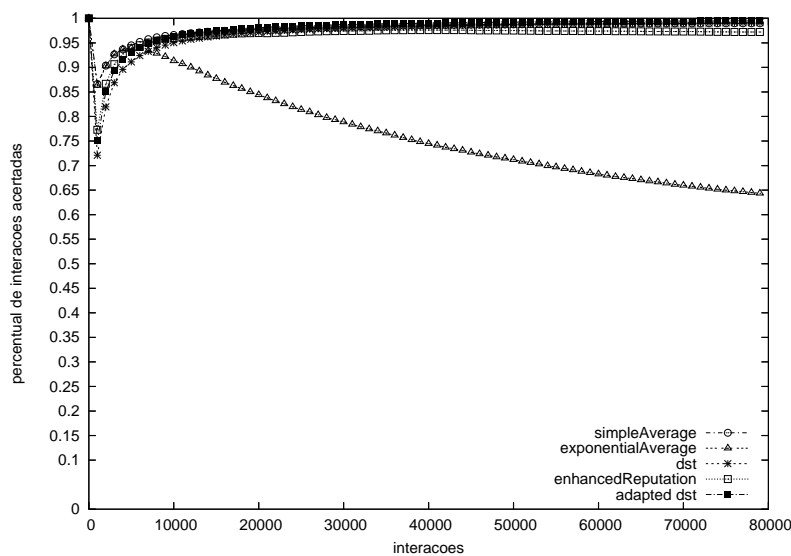


Figura 1. Percentual médio de decisões acertadas.

O primeiro teste considerou provedores bons com 90% de chance de atender a uma

requisição e provedores maus com 10% de chance. A Figura 1 mostra que o mecanismo exponentialAverage tem uma queda brusca nas decisões acertadas. A rápida convergência deste método faz com que poucas falhas de um provedor bem comportado causem uma grande redução no valor de sua reputação, levando-o a ser julgado como mau. Clientes que fizeram esse tipo de mau julgamento disseminarão baixos valores de reputação para bons provedores. *Peers* que não conhecem ainda esses bons provedores, ao receberem o testemunho destes clientes, se basearão nestas informações e decidirão erradamente não fazer interação. Cada falha que um bom provedor tiver, poderá fazer com que mais um cliente passe a acreditar e divulgar que ele é mal comportado. À medida que isso vai acontecendo ao longo da simulação, o percentual de decisões acertadas vai reduzindo.

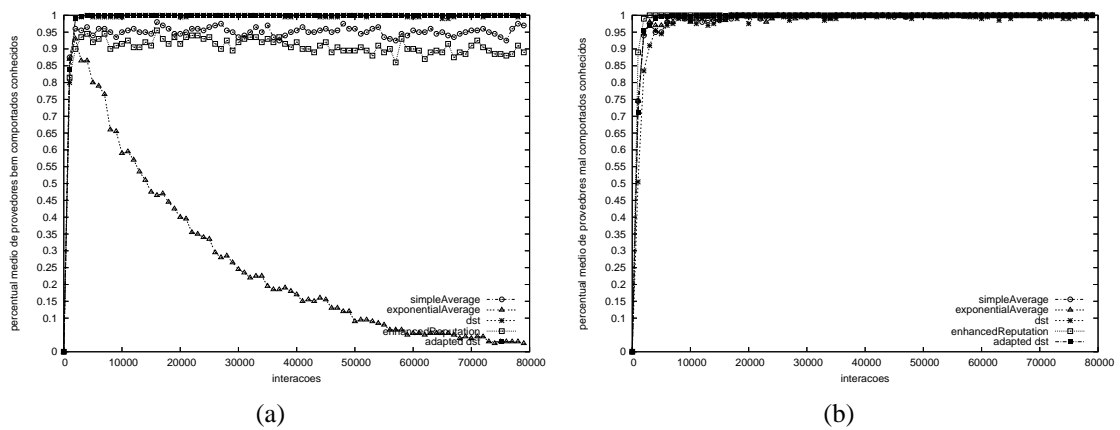


Figura 2. (a) Percentual médio de provedores bem comportados que são conhecidos; (b) Percentual médio de provedores mal comportados que são conhecidos

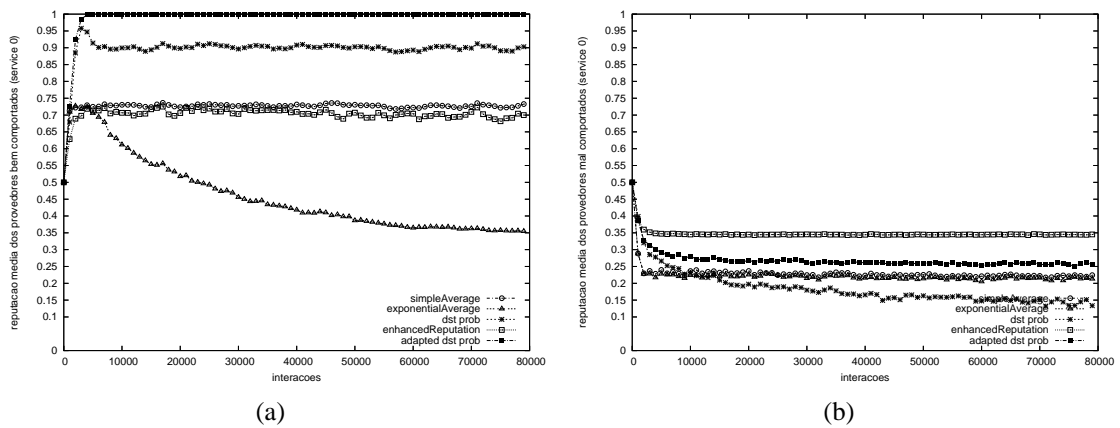


Figura 3. (a) Reputação média dos provedores bem comportados; (b) Reputação média dos provedores mal comportados;

A Figura 2(a) mostra uma queda brusca do método exponentialAverage, em virtude dos maus julgamentos já citados. Esse gráfico também mostra que o método enhancedReputation atinge, ao longo da simulação, percentuais mais baixos de bons provedores conhecidos se comparado aos outros métodos. Entretanto, observa-se que este método não foi afetado da mesma forma que o exponentialAverage. Apesar de ambos os mecanismos

usarem o fator de decaimento, que dá mais peso às avaliações mais recentes, o `exponentialAverage` se diferencia do `enhancedReputation` porque considera, para o cálculo da reputação, histórico com tamanho limitado das últimas avaliações. Isso significa que não importa como o provedor agiu ao longo de sua história, somente as H últimas iterações são consideradas. O método `enhancedReputation` não trabalha com histórico de avaliações recentes, e por isso tem uma convergência mais lenta.

No segundo teste, foi configurada uma probabilidade de 0.25 do cliente não conseguir avaliar o provedor depois de uma interação. O objetivo é verificar se numa situação como esta, a incerteza mapeada pelo método DST oferece vantagem (vide Seção 4.3). Como este cenário é semelhante ao anterior, serão incluídos neste documento, por limitações de espaço, apenas os gráficos mais relevantes.

As Figuras 5(a) e 5(b) mostram que quase todos os métodos apresentaram um comportamento diferente neste cenário. Os valores médios de reputação dos provedores bons e o percentual destes provedores identificados como bons foram reduzidos. Isso ocorre porque estes provedores têm 25% de chance de receberem avaliação neutra e, com isso, o valor final da reputação destes provedores pode descer abaixo do limite (seção 4.3) usado para que ele seja considerado bem comportado.

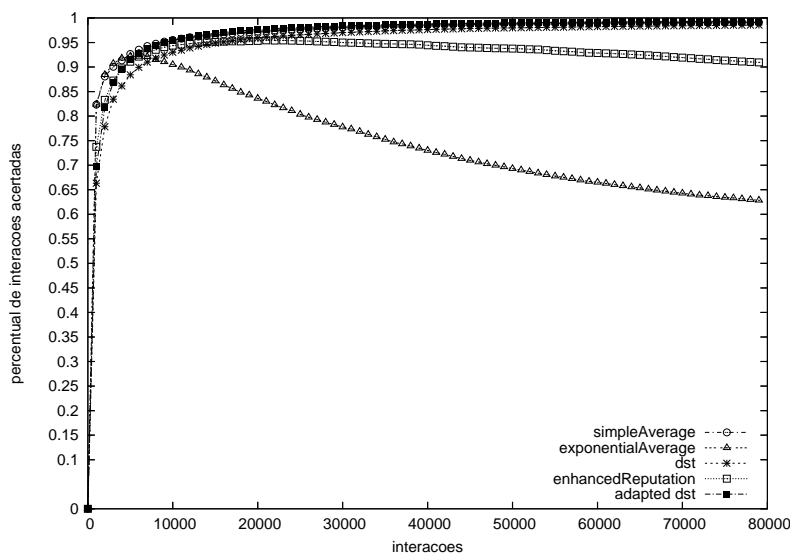


Figura 4. Percentual médio de decisões acertadas.

O `enhancedReputation` foi mais afetado neste cenário. O gráfico da Figura 5(a) mostra que a reputação média dos provedores bem comportados apresenta uma queda ao longo da simulação. O mesmo acontece com o percentual de provedores bons conhecidos, mostrado no gráfico da Figura 5(b). A Figura 4 mostra uma queda no percentual médio de decisões acertadas. Isso porque, além da possibilidade de poucas falhas de provedores bem comportados causarem seu mau julgamento, existem as interações onde o cliente não consegue avaliar os provedores e associa a eles uma avaliação neutra. Isso faz com que em algumas oportunidades, onde provedores bem comportados poderiam mostrar sua capacidade de bom atendimento, sejam julgados com um valor neutro.

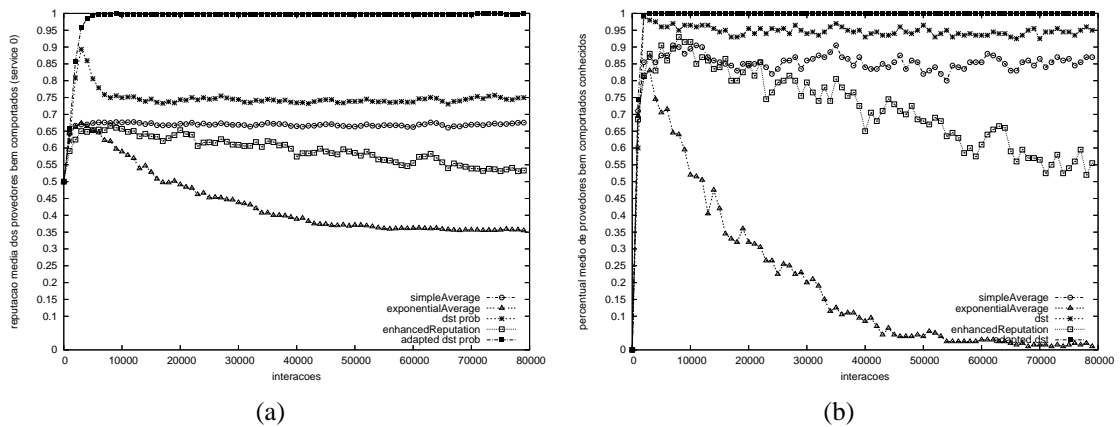


Figura 5. (a)Reputação média dos provedores bem comportados; (b)Percentual médio de provedores bem comportados que são conhecidos.

O mecanismo DST não apresentou grandes vantagens se comparado com métodos que não tratam incerteza de maneira especial. Somente o método adaptedDST não teve seu desempenho alterado e surpreende sendo o único método a conseguir, neste cenário, a se manter identificando um percentual médio próximo de 100% de provedores bons que são conhecidos. O mapeamento da incerteza representou uma vantagem neste cenário, mas somente quando foi usada a agregação das informações de primeira e segunda mão através da regra de combinação de DST.

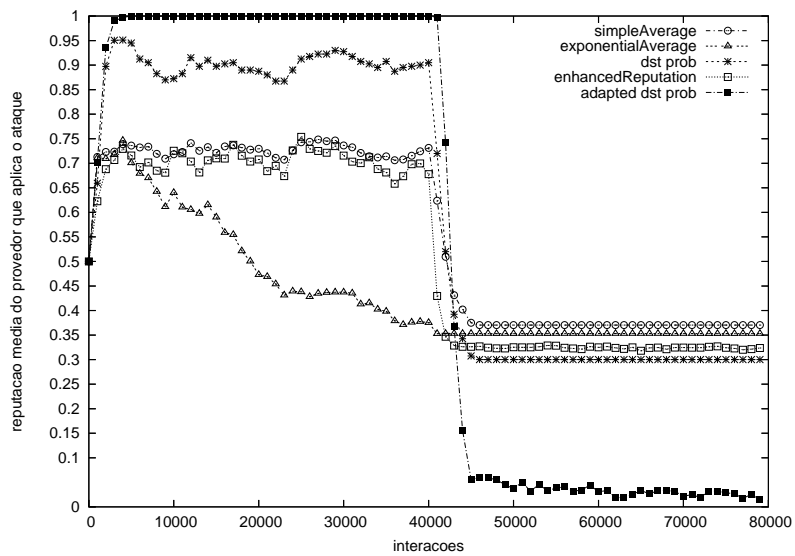


Figura 6. Reputação média do provedor que aplica o ataque da mudança repentina de comportamento

O terceiro teste considera que um dos provedores aplicará o ataque da mudança repentina de comportamento, alterando seu comportamento de bom para mau no meio da simulação. Mostraremos, por limitações de espaço, somente a reputação média do provedor que aplica o ataque (Figura 6). É possível notar que todos os métodos detectam rapidamente a mudança de comportamento. Sendo assim, fica demonstrado que convergência

muito rápida trazida pelos métodos exponenciais não apresenta uma vantagem contra o ataque da mudança repentina de comportamento e, além disso, apresenta as desvantagens demonstradas pelos cenários anteriores.

4.7. Conclusão

Neste trabalho, foram mostrados importantes resultados da fase inicial do estudo dos métodos de cálculo da reputação. Foi observado que o uso do fator de decaimento (*fading factor*) para aumentar convergência, usado pelos métodos exponenciais, não representa uma grande vantagem nos cenários com provedores que aplicam o ataque da mudança repentina de comportamento. Métodos que não utilizam este artifício já apresentam uma reação rápida a este tipo de ataque.

Os testes demonstraram que o aumento da convergência representou, na realidade, uma desvantagem já que nos ambientes reais, provedores bem comportados não são infalíveis e podem, em alguns momentos, não conseguir atender a requisição de algum serviço/recurso. O uso do fator de decaimento, dando maior importância às experiências mais recentes, faz com que poucas falhas consecutivas de um provedor bom não sejam toleradas e ele passe a ser julgado como mal comportado. Quanto maior o fator de decaimento, maior a convergência e menor a tolerância a falhas. O caso do método *exponentialAverage* se mostrou ainda mais grave porque além de usar o fator de decaimento, este método só considera as H últimas interações, ou seja, associa um peso nulo ao comportamento que o provedor teve nas interações anteriores a estas H últimas.

Também foi observado que toda a complexidade do método DST não o fez ganhar muito em desempenho em relação a métodos mais simples como o *simpleAverage*, nem mesmo no cenário onde foi inserida a incerteza através da probabilidade de falha na avaliação. Já o mecanismo *adaptedDST* conseguiu demonstrar um bom desempenho em todos os cenários e um melhor desempenho no cenário com incerteza.

4.8. Trabalhos Futuros

A próxima versão do simulador, já em desenvolvimento, incluirá a possibilidade de simular mecanismos que usem método Bayesiano, apresentado em propostas como, por exemplo, [Wang 2003], [Wang and Vassileva 2003], [Buchegger and Boudec 2004] e [Buchegger and Boudec 2005]. Essa versão também será capaz de gerar um cenário diferente do apresentado neste trabalho, que simulará o ambiente de aplicações de compartilhamento de arquivos (*file-sharing*) com o objetivo de estudar o comportamento das propostas quando usadas dentro da mais famosa aplicação P2P dos dias atuais.

O simulador também permitirá testar os mecanismos em cenários mais hostis, como por exemplo, *peers* praticando o ataque do testemunho mentiroso. Serão implementadas algumas propostas de mecanismos de credibilidade e estas serão testadas em conjunto com os mecanismos de reputação. Além de testar que mecanismos de credibilidade são mais eficazes na detecção de *peers* mentirosos, será possível saber quais as combinações de mecanismos de reputação e credibilidade são mais robustas nestes ambientes.

Referências

Adar, E. and Huberman, B. (2000). Free riding on gnutella.

- Asvanund, A., Clay, K., Krishnan, R., and Smith, M. D. (2004). An empirical analysis of network externalities in peer-to-peer music-sharing networks. *Information Systems Research*, 15(2):155–174.
- Buchegger, S. and Boudec, J.-Y. L. (2004). A robust reputation system for p2p and mobile ad-hoc networks. In *Second Workshop on Economics of Peer to Peer Systems*.
- Buchegger, S. and Boudec, J.-Y. L. (2005). Self-policing mobile ad-hoc networks by reputation systems. *IEEE Communications Magazine*.
- Damiani, E., di Vimercati, D. C., Paraboschi, S., Samarati, P., and Violante, F. (2002). A reputation-based approach for choosing reliable resources in peer-to-peer networks. In *Proceedings of the 9th ACM conference on Computer and communications security*.
- Hughes, D., Coulson, G., and Walkerdine, J. (2005). Free riding on gnutella revisited: The bell tolls? *IEEE Distributed Systems Online*, 6(6):1.
- Jøsang, A., Ismail, R., and Boyd, C. (2005). A survey of trust and reputation systems for online service provision (to appear). *Decision Support Systems*.
- KaZaA. <http://www.kazaa.com/>.
- Liu, J. and Issarny, V. (2004). Enhanced reputation mechanism for mobile ad hoc networks. In *Proceedings of iTrust 2004*, pages 48–62.
- Saroiu, S., Gummadi, P. K., and Gribble, S. D. (2002). A measurement study of peer-to-peer file sharing systems. In *Proceedings of Multimedia Computing and Networking (MMCN 02)*.
- Sentz, K. (2002). *Combination of Evidence in Dempster-Shafer Theory*. PhD thesis, SNL, LANL, and Systems Science and Industrial Eng. Dept., Binghamton Univ.
- Wang, Y. (2003). Bayesian network-based trust model in peer-to-peer networks. In *Proceedings of Workshop on Deception, Fraud and Trust in Agent Societies at the Autonomous Agents and Multi Agent Systems 2003 Conference (AAMAS-03)*.
- Wang, Y. and Vassileva, J. (2003). Trust and reputation model in peer-to-peer networks. In *Proceedings of Third International Conference on Peer-to-Peer Computing, 2003. (P2P 2003)*.
- Yu, B. and Singh, M. (2002a). Distributed reputation management for electronic commerce. In *Computational Intelligence*, volume 18, pages 535–549.
- Yu, B. and Singh, M. (2002b). An evidential model of distributed reputation management. In *Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems*.
- Yu, B. and Singh, M. (2003). Detecting deception in reputation management. In *Proceedings of AAMAS03*.
- Yu, B., Singh, M., and Sycara, K. (2004). Developing trust in large scale peer-to-peer systems. In *Proceedings of First IEEE Symposium on Multi-Agent Security and Survivability*.