Influência do Ataque do Testemunho Mentiroso nos Modelos de Reputação *

Fabiana Martins da Silva[1], **José Ferreira de Rezende**[1]

[1]Grupo de Teleinformática e Automação (GTA) – COPPE
Universidade Federal do Rio de Janeiro (UFRJ)

{fabiana,rezende}@gta.ufrj.br

Abstract. *The lying witness attack to the reputationm-based cooperation incentive schemes happens when a peer asks for information about a provider for a witness who answers with false information that would influenciate him to interact with a misbehaved provider or to prevent him to interact with a good provider. Besides to an isolated action, lying witnesses may form a collusion to increase the harm caused by their attack. This work analyses how each reputation-based mathematic method is sensitive to this attack and dependent of an extra mechanism, i.e. credibility mechanisms, to guarantee a better performance in environments where this attack may occur.*

Resumo. *O ataque do testemunho mentiroso aos mecanismos de incentivo à cooperação baseados em reputação acontece quando um peer requisita informações a respeito de um provedor a uma testemunha e esta fornece falsas informações, para influenciá-lo a interagir com um provedor mal comportado ou a deixar de interagir com um bem comportado. Além de agir isoladamente, testemunhas mentirosas podem formar conluio e aumentar os prejuízos causados por este ataque. Este trabalho estuda como cada método matemático de cálculo da reputação é sensível a este ataque e dependente de um mecanismo adicional, como os mecanismos de credibilidade, para tentar garantir um melhor funcionamento em ambientes onde este ataque possa estar presente.*

1. Introdução

As redes P2P (*Peer-to-Peer*) baseiam seu funcionamento em um importante fundamento: a cooperação entre os *peers* que as constituem. Cada *peer* desempenha tanto o papel de cliente quanto o de servidor e, assim, é possível compartilhar os mais variados tipos de recursos e serviços como, por exemplo, arquivos, ciclos de CPU, etc. Entretanto, estudos como [Saroiu et al. 2002], [Adar and Huberman 2000], [Asvanund et al. 2004] e [Hughes et al. 2005] demonstraram que existe um grande número de usuários de aplicações em redes P2P que não obedece a esta premissa de funcionamento, comprometendo então o bom funcionamento destes sistemas.

Esses usuários mal comportados se dividem em dois grupos, os egoístas (*free riders*), que usam recursos de outros *peers*, mas não tornam seus próprios recursos disponíveis ou limitam muito seu acesso; e os maliciosos, que prejudicam a rede, não para o benefício próprio (economia de recursos), mas apenas para prejudicar outros usuários.

*Este trabalho recebeu recursos do CNPq, CAPES, FAPERJ e FINEP.

A existência destes *peers* estimulou o estudo de mecanismos de incentivo a cooperação e uma das principais linhas de pesquisa explora o 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. Esta medida de reputação calculada e associada a cada *peer* será usada nos momentos de requisitar e oferecer serviços/recursos. 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.

O trabalho publicado em [da Silva and de Rezende 2007] iniciou um estudo de comparação entre vários métodos matemáticos adotados no cálculo da reputação por diferentes mecanismos de cooperação. Foi estudada a eficiência de cada mecanismo em detectar quais provedores presentes na rede são cooperativos e quais não são. Também foi analisada a convergência de cada método, ou seja, quais detectavam mais rapidamente quando aconteciam mudanças repentinas de comportamento de provedores. Entretanto, [da Silva and de Rezende 2007] considerou que os *peers* que trocavam informações entre si para o cálculo da reputação dos provedores não mentiam a respeito de suas experiências.

Tendo em vista que o ataque do testemunho mentiroso é um conhecido ataque aos mecanismos de incentivo à cooperação baseados em reputação, o trabalho desenvolvido por este artigo dá continuidade ao trabalho anterior, avaliando os métodos através da simulação dos mesmos em ambientes onde este ataque esteja sendo praticado. Neste trabalho, também serão apresentados e testados novos métodos, que ainda não estavam implementados na versão anterior do simulador usada em [da Silva and de Rezende 2007].

O artigo está organizado da seguinte forma. Na Seção 2, é descrito o ataque estudado neste artigo e a sua formulação matemática. Em seguida, a Seção 3 descreve os métodos matemáticos usados para o cálculo da reputação. Na Seção 4, são descritos os cenários de simulação e na Seção 5 são apresentados os resultados obtidos. Finalmente, a Seção 6 apresenta as conclusões e fornece diretrizes para a continuidade deste trabalho.

2. O Ataque do Testemunho Mentiroso

Numa rede P2P diz-se que dois *peers* interagem quando um deles requisita ao outro algum serviço/recurso. Ao término de uma interação, o *peer* que requisitou o serviço/recurso avalia o comportamento do *peer* com o qual interagiu e armazena esta avaliação. Cada participante da rede mantém históricos de avaliações geradas a partir de suas experiências com outros participantes, chamadas de "informações de primeira mão". Os *peers* da rede podem usar as informações de primeira mão que possuem a respeito de outros *peers* para calcular seus valores de reputação, entretanto, em uma rede com muitos usuários 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. Por causa disso, os *peers* trocam experiências entre si. Informações recebidas de outros *peers*, geradas a partir das interações das quais eles participaram, são chamadas de informações de segunda mão.

O ataque do testemunho mentiroso acontece quando um *peer*, ao receber requisições de informações a respeito de um provedor responde com um testemunho diferente das experiências que teve com este provedor. A testemunha pode fazer parecer que suas experiências foram melhores que as reais com o objetivo de beneficiar o provedor ou prejudicar o cliente que requisitou a informação, tentando induzi-lo a interagir com

um mal provedor. A mentira também pode fazer com que as experiências da testemunha pareçam piores que as reais para difamar o provedor ou influenciar o cliente a perder a chance de interagir com um bom provedor. Neste caso, a testemunha pode ter interesse em afastar clientes deste provedor para evitar a concorrência pelos seus recursos. O ataque pode ainda ser gratuito, simplesmente para causar o mau funcionamento da rede P2P.

O artigo [Yu and Singh 2003] apresentou três modelos matemáticos que podem ser usados, por uma testemunha mentirosa para manipular suas informações de primeira mão antes de repassá-las ao *peer* que as requisitou:

- Exagero Positivo: expressa experiências com o provedor melhores que as reais.

$$y = \alpha + x - \alpha * x \tag{1}$$

- Exagero Negativo - expressa experiências com o provedor piores que as reais.

$$y = x - \alpha * x/(1 - \alpha) \tag{2}$$

- Mentira Complementar - expressa experiências com o provedor opostas às reais.

$$y = 1 - x \tag{3}$$

  onde x é a informação de primeira mão que a testemunha mentirosa possui do provedor, y é a informação de primeira mão manipulada, ou seja, o testemunho mentiroso e α é uma constante, que assume o valor 0.4 neste trabalho.

Este valor de α foi escolhido de maneira que as testemunhas que estejam exagerando positivamente consigam transformar qualquer valor de informação de primeira mão num valor dentro de um intervalo que faça parecer que o provedor agiu de maneira comportada. Esse valor de α também faz com que as testemunhas que estejam exagerando negativamente consigam sempre transformar suas informações de primeira mão em informações dentro do intervalo de valores indicativo de mal comportamento.

Um *peer* pode praticar isoladamente o ataque do testemunho mentiroso ou pode se unir a um grupo de outros *peers*, com os quais estabelece acordos para praticar o ataque em conluio. Participantes de um grupo de conluio difamam *peers* que não estejam no grupo e elogiam *peers* que façam parte do grupo.

Existem inúmeras propostas de mecanismo de credibilidade para serem usados em conjunto com os mecanismos de reputação com o objetivo de tornar cada *peer* capaz de calcular um valor que expresse a honestidade de cada um dos outros *peers* da rede de quem já requisitou informações de segunda mão. Entretanto, a adoção destes mecanismos significa que cada *peer* da rede deverá calcular, manter atualizado e armazenar dados a respeito de cada um dos *peers* de quem requisitar o testemunho. Tudo isso acrescenta maior complexidade, maior processamento e maior necessidade de memória, reduzindo assim os benefícios trazidos pela adoção dos métodos de reputação.

Sendo assim, torna-se muito importante entender a influência do ataque do testemunho mentiroso nos métodos matemáticos de reputação, perceber o quanto eles são sensíveis a este ataque e o quanto são dependentes de um mecanismo de credibilidade para o bom funcionamento. Para isso, os mecanismos serão testados em ambientes com testemunhas mentirosas sem usar nenhuma proteção de algum mecanismo adicional, ou seja, o valor de credibilidade que cada *peer* associará a cada testemunha será sempre 1.

3. Descrição dos Métodos Matemáticos

3.1. Média Simples - simpleAverage

Considerando 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:

$$R(P_i, P_j) = \begin{cases} \sum_{k=1}^{h} e_{ij}^k / \ h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases} \tag{4}$$

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. A agregação das informações de segunda mão é dada por:

$$T(P_i, P_j) = \begin{cases} \sum_{k=1}^{L} w_k * R(W_k, P_j) / \ L & \text{if } L \neq 0; \\ 0.5 & \text{if } L = 0. \end{cases} \tag{5}$$

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 assumirá o valor 1 nas simulações deste trabalho. Por fim, a seguinte função é usada para o cálculo do valor final de reputação, agregando informações de primeira e segunda mão:

$$Rep(P_i, P_j) = \eta * R(P_i, P_j) + (1 - \eta) * T(P_i, P_j) \tag{6}$$

onde, $\eta = h/H$. Portanto, quando o histórico de avaliações estiver cheio (h=H), a informação de segunda mão não será considerada no cálculo do valor final de reputação.

3.2. Média Simples Adaptada - adaptedSimpleAverage

O método de média simples descrito na subseção 3.1 só usa informações de segunda mão enquanto seu histórico não estiver cheio. Nesta subseção, apresenta-se uma pequena adaptação, cujo comportamento será estudado durante as simulações, onde o método sempre utiliza a informação de segunda mão para o cálculo do valor final da reputação.

Sendo assim, as informações de primeira mão serão agregadas pela equação 4 e as informações de segunda mão serão agregadas pela equação 5. Para o cálculo final da reputação de um provedor P_j, um *peer* cliente P_i usará a seguinte equação:

$$Rep(P_i, P_j) = \zeta * R(P_i, P_j) + (1 - \zeta) * T(P_i, P_j) \tag{7}$$

onde, ζ será uma constante no intervalo $[0, 1]$.

3.3. Média Exponencial - exponentialAverage

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

$$R(P_i, P_j) = \begin{cases} (1-\gamma)^{(h-1)} * e_{ij}^1 + (1-\gamma)^{(h-2)} * \gamma * e_{ij}^2 + ... + (1-\gamma)^0 * \gamma * e_{ij}^h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases} \tag{8}$$

onde γ, variável chamada comumente de fator de decaimento ou mesmo pelo termo em inglês *fading factor*, pode assumir qualquer valor dentro do intervalo $[0, 1]$, o valor 0.6 é

adotado neste trabalho. 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, é capaz de armazenar H avaliações mais recentes.

Este método usa as fórmulas descritas na subseção 3.1 para agregar as informações de segunda mão (equação 5) e para o cálculo final da reputação (equação 6).

3.4. Média Exponencial Adaptado - adaptedExponentialAverage

O mecanismo exponentialAverage (seção 3.3) só usa informações de segunda mão enquanto seu histórico não estiver cheio. O método exponencial adaptado sempre considerará as informações de segunda mão no cálculo final da reputação. Um cliente agregará as informações de primeira usando a equação 8 e agregará as informações de segunda mão utilizando a equação 5. O valor final da reputação será calculado pela equação 7.

3.5. Método Exponencial sem utilização de Histórico - enhancedReputation

O trabalho [Liu and Issarny 2004] apresenta um mecanismo de cálculo de reputação que não usa histórico de avaliações. A cada interação entre *peers*, a seguinte função é usada:

$$R(P_i, P_j) = (1 - \gamma) * R(P_i, P_j)_{current} + \gamma * e_{ij} \tag{9}$$

onde γ, é o fator de decaimento ou *fading factor* (vide Seção 3.3). $R(P_i, P_j)_{current}$ 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:

$$T(P_i, P_j) = \frac{\sum_{k=1}^{L} w_k * R(W_k, P_j)}{\sum_{k=1}^{L} w_k} \tag{10}$$

onde L é o número de testemunhas e w_k é a credibilidade dada à informação de segunda mão recebida da testemunha W_k. w_k assume o valor 1 nas simulações executadas neste trabalho. Por fim, a equação 7 é usada para o cálculo do valor final de reputação, agregando informações de primeira e segunda mão.

3.6. Método da Teoria de Dempster-Shafer - dst

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. 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. Enquanto P_i não tem experiências com P_j, $m(T, notT) = 1$ e as demais crenças assumem

o valor 0. A medida que P_i tem oportunidades de interagir e avaliar P_j, suas crenças são atualizadas e a incerteza vai dando lugar a maior crença em alguma das hipótese de θ.

A DST também define uma regra de combinação 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:

$$m_{rs}(T) = \frac{m_r(T) * m_s(T) + m_r(T) * m_s(T, notT) + m_r(T, notT) * m_s(T)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \quad (11)$$

$$m_{rs}(notT) = \frac{m_r(notT) * m_s(notT) + m_r(notT) * m_s(T, notT) + m_r(T, notT) * m_s(notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \quad (12)$$

$$m_{rs}(T, notT) = \frac{m_r(T, notT) * m_s(T, notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \quad (13)$$

Neste trabalho o método da teoria de Dempster-Shaffer é estudado como método de cálculo da reputação tomando como base as proposta dos artigos [Yu and Singh 2002a], [Yu and Singh 2002b] e [Yu and Singh 2003]. Primeiramente, assume-se que os clientes sempre avaliam os provedores com um dos 11 valores discretos $\{$0.0; 0.1; 0.2; ...1.0 $\}$. Depois, considera-se a função

$$f(x_k) = g/\ H \quad (14)$$

onde x_k é um dos 11 valores discretos de avaliação, g é a quantidade de avaliações que assumem o valor x_k. O histórico é capaz de armazenar H avaliações mais recentes.

Para o cálculo das informações de primeira mão, são considerados dois valores limites, ω e Ω, onde $0 \leq \omega \leq \Omega \leq 1$ e cujos valores adotados neste trabalho são $\omega = 0.4$ e $\Omega = 0.6$. Assim, as crenças $m(T)$, $m(notT)$ e $m(T, notT)$ relacionadas ao comportamento de um *peer* P_j podem ser calculadas por:

$$m(T) = \sum_{x_k=\Omega}^{1} f(x_k) \quad m(notT) = \sum_{0}^{x_k=\omega} f(x_k) \quad m(T, notT) = \sum_{x_k=\omega}^{x_k=\Omega} f(x_k) \quad (15)$$

As informações de segunda mão, que neste caso, são as crenças relacionadas ao comportamento de P_j, calculadas e informadas a P_i por outros *peers*, são agregadas através da regra de combinação de DST (equações 11, 12 e 13). Nas propostas dos trabalhos [Yu and Singh 2002a], [Yu and Singh 2002b] e [Yu and Singh 2003], a informação de primeira mão **não** é agregada à informação de segunda mão. Uma vez que P_i possua seu histórico de avaliações de P_j cheio, ele considera apenas as crenças que ele próprio calcula. Enquanto isso, considera apenas as informações de segunda mão agregadas pela regra de combinação de DST.

3.7. Método Adaptado da Teoria de Dempster-Shafer - adaptedDst

Este mecanismo é uma adaptação do mecanismo DST. O cálculo das crenças a partir das informações de primeira mão são executados pelas equações 14 e 15 e o cálculo

das crenças agregadas de segunda mão são executados através da regra de combinação de Dempster-Shafer (equações 11, 12 e 13). Entretanto, neste método, 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.

3.8. Método de Bayes - bayes

Neste trabalho, o método Bayesiano será estudado através de um mecanismo baseado na proposta de [Buchegger and Boudec 2004]. Considere dois *peers* P_i e P_j e um parâmetro θ_{ij} que representa a probabilidade com a qual P_i "acha" que P_j irá se comportar bem. Inicialmente, θ_{ij} é desconhecido e assume a forma de uma distribuição *a priori* $Beta(1,1)$. Depois, a cada nova interação que acontece entre estes *peers*, os valores α e β da distribuição $Beta(\alpha,\beta)$ são atualizados através das seguintes equações:

$$\alpha_{ij} = \alpha_{ij} + s \quad \beta_{ij} = \beta_{ij} + f \tag{16}$$

onde s é o número de interações de sucesso e f o número de interações falhas que P_i teve com P_j. As informações de primeira mão que P_i guarda de P_j são os valores de α_{ij} e β_{ij}. No que se refere à agregação das informações de segunda mão, as seguintes equações são usadas:

$$\alpha_w = \sum_{k=1}^{L} w_k * \alpha_{kj} \quad \beta_w = \sum_{k=1}^{L} w_k * \beta_{kj} \tag{17}$$

onde L é o número de testemunhas, α_w e β_w são os valores resultantes da agregação dos parâmetros α_{kj} e β_{kj}, que são as informações dadas por cada testemunha W_k a respeito de P_j. w_k é a credibilidade associadas às informações de segunda mão e assume sempre o valor 1 nas simulações deste trabalho.

Quanto ao cálculo final da reputação, é feito através das seguintes equações:

$$\alpha_f = \alpha_{ij} + \alpha_w \quad \beta_f = \beta_{ij} + \beta_w \quad \theta_{ij} = \mathbb{E}(Beta(\alpha_f, \beta_f)) \tag{18}$$

onde α_f e β_f são os valores finais de α e β, usados no cálculo de θ_{ij}

3.9. O Uso da Reputação Calculada

Nos mecanismos das seções 3.1, 3.2, 3.3, 3.4 e 3.8, a reputação calculada para um *peer* é representada por um valor dentro de um intervalo $[0,1]$. No mecanismo da seção 3.5, a reputação deve estar no intervalo $[-1,1]$. Em todos estes casos, a reputação pode simplesmente ser comparada com valores limites no momento de concluir se um dado *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.

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:

$$prob(T) = \frac{m(T) + m(T, notT)}{1 + m(T, notT)} \tag{19}$$

4. O simulador

Para a avaliação do ataque de testemunho mentiroso e a sua influência nos esquemas baseados em reputação, foi desenvolvido um simulador em linguagem C que permite criar cenários *peer-to-peer*, realizar as interações entre os *peers* aplicando os métodos de cálculo de reputação descritos anteriormente, e gerar ataques de falso testemunho isolados ou através de conluios.

4.1. A Geração de Cenários

O tempo de duração de cada simulação é configurado pela definição do número de interações entre clientes e provedores. As simulações deste trabalho são compostas de 120000 interações. O cenário considerado é constituído de 100 *peers*, 10 dos quais são unicamente provedores e 90 unicamente clientes. 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. Esta probabilidade está configurada com o valor de 0.9 para os provedores bem comportados e com o valor 0.1 para os mal comportados. 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.

A quantidade de clientes que atuam como testemunhas em cada interação é 5. A quantidade total de clientes da rede que praticarão o ataque do testemunho mentiroso e o modelo matemático que será usado (seção 2) são parâmetros configurados conforme o interesse de cada simulação. Quanto ao ataque da mentira em conluio, numa rede P2P real, a formação de conluio é muito interessante para *peers* mal comportados, pois, os *peers* em conluio, sempre testemunham elogiando os *peers* do grupo e difamando aqueles que não participam do conluio. No simulador, o conluio é simulado de duas formas. Primeiramente, através da configuração de um grupo de conluio onde os clientes usam exagero positivo para elogiar os provedores mal comportados e exagero negativo para difamar os provedores bem comportados. Depois, através de um grupo de clientes que usam mentira complementar para difamar bons provedores elogiar os maus.

O algoritmo de geração do cenário define, através de escolha aleatória, quais *peer* serão clientes, quais serão provedores, quais provedores serão bem e quais serão mal comportados, quais testemunhas serão honestas e quais serão desonestas. São escolhidos aleatoriamente o cliente, o provedor e as testemunhas que irão participar de cada interação. Durante a geração de cenário, os *peer* escolhidos para serem provedores, suas respectivas informações de comportamento, as testemunhas escolhidas para atuarem como mentiro-

sas e as informações relacionadas a cada interação (cliente, provedor e testemunhas escolhidas) são gravadas em arquivos possibilitando que o mesmo cenário possa ser usado em diversas simulações com diversos métodos matemáticos de cálculo da reputação.

4.2. Simulação dos Métodos

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 mecanismo bayes, cuja é 1 em caso de sucesso, e no caso do mecanismo da seção 3.5, cujo valor deve ser 0.2 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 o bayes, cuja avaliação deve ser 0 em caso de falha, e no caso do mecanismo da seção 3.5, cujo valor considerado e -0.2.

Uma reputação abaixo de 0.4 indica mau comportamento e uma acima de 0.6 bom comportamento. No método da seção 3.5 estes valores são respectivamente -0.2 e 0.2. Uma reputação 0,5 é associada a um provedor novo ou desconhecido, para o qual não se calculou nenhum valor de reputação. No mecanismo da seção 3.5, este valor é zero.

Antes da simulação dos métodos num dado cenário, o simulador gera um arquivo com um resultado (sucesso ou falha) e uma correspondente avaliação a ser dada pelo cliente, para cada interação. Durante a simulação de cada método, cada vez que o cliente decidir, baseado na análise da reputação do provedor, requisitá-lo o serviço desejado, o resultado e a avaliação da interação serão lidos deste arquivo. Isso garante que todas as interações que forem consumadas durante a simulação de cada método terão os mesmos cliente, provedor, resultado e avaliação. A diferença estará justamente na decisão de consumar ou não a interação, que será tomada pelo cliente, baseada na reputação calculada pelo método matemático em uso. Isso permite observar que método(s), em cada cenário, causa(m) um número maior de decisões acertadas. Um *peer* toma uma decisão acertada toda vez decide não interagir com um mau provedor ou interagir com um bom provedor.

5. Resultados

O primeiro conjunto de testes considerou cenários com testemunhas mentirosas agindo isoladamente, sem formar conluio. Os três modelos matemáticos para mentira, exagero positivo, exagero negativo e mentira complementar, foram testados. Inicialmente, considerou-se históricos de avaliações armazenados pelos *peers* com capacidade para 100 avaliações. Também foi definido que os métodos que fazem uso da equação 7 para o cálculo final da reputação (adaptedSimpleAverage, adaptedExponentialAverage e enhancedReputation), adotaram o valor 0.5 para a constante ζ, ou seja, atribuíram pesos iguais às informações de primeira e segunda mão. Na figura 1(a) é possível perceber que, no modelo de exagero positivo, o mecanismo de média simple e o mecanismo exponencial adaptados e o mecanismo exponencial sem histórico, que sempre atribuem o mesmo peso às informações de segunda mão, têm um desempenho melhor que o mecanismo de média simples e o exponencial originais, que iniciam a simulação dando um peso muito grande às informações de segunda mão e diminuem este peso conforme o preenchimento dos históricos de avaliações. Comparando as figuras 1(a) e 1(b) percebe-se que, a partir de um certo número de testemunhas mentirosas presentes na rede, o exagero negativo tem uma influência bem maior que a do exagero positivo.

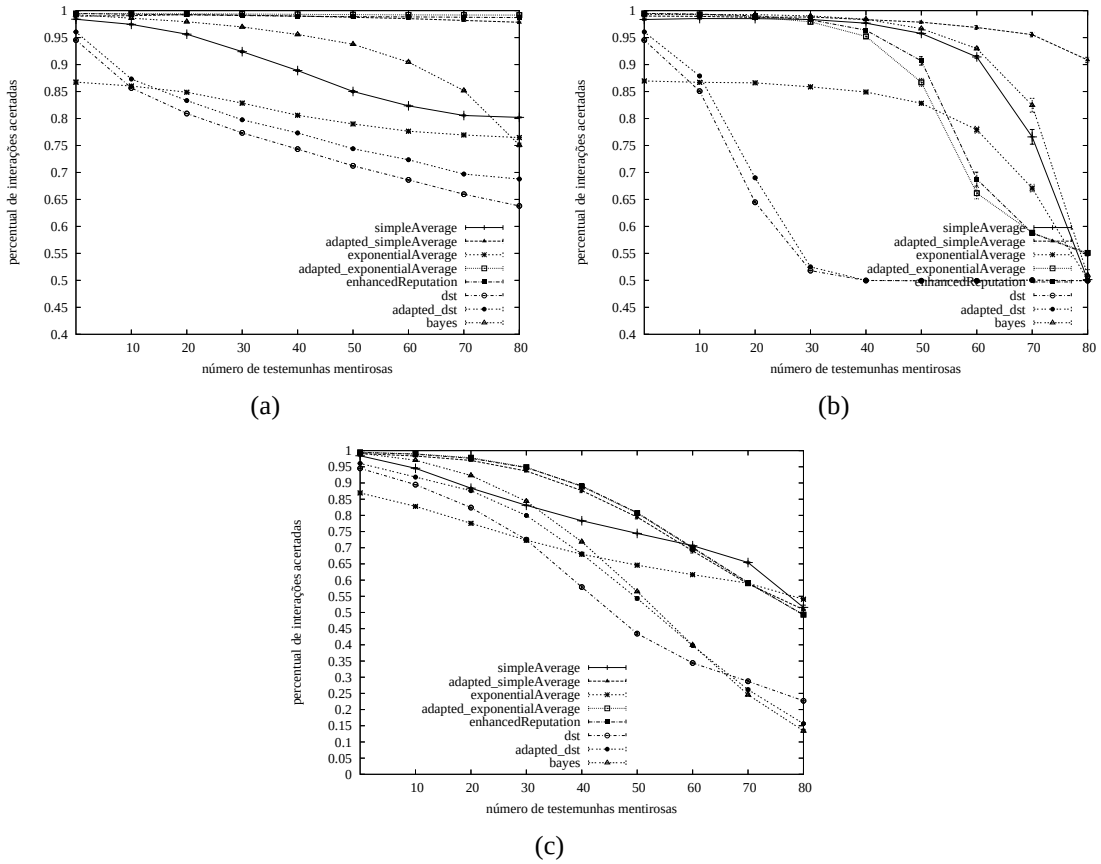

Figura 1. (a)Exagero positivo; (b)Exagero negativo (c)Mentira Complementar

O exagero positivo pode fazer com que alguns clientes se enganem e decidam interagir com *peers* que são mal comportados, mas quando estes clientes acumulam informações de primeira mão essas decisões erradas são evitadas. Entretanto, com exagero negativo, o erro ao qual os clientes são induzidos é o de não interagir com provedores bons. Sem interagir não há como adquirir experiência e as informações de segunda mão continuarão sendo a principal fonte de informações para as tomadas de decisão.

A figura 1(c) mostra que o modelo de mentira complementar exerce maior influência nos métodos. Isso acontece porque a testemunha que usa mentira complementar repassa ao cliente uma visão completamente oposta a que tem da realidade e não somente aproxima, através de um exagero, o comportamento do provedor para mais ou para menos bem comportado. Para aumentar a influência dos modelos de exagero é necessário aumentar o valor da constante α (equações 1 e 2). As simulações foram repetidas considerando o valor 0.6 para a constante ζ, ou seja, um com maior peso dado às informações de primeira mão. A figura 2(a) não mostra melhora de desempenho para o modelo exagero positivo pois, como já tinha sido visto na figura 1(a), este modelo não tem influência significativa nos métodos que usam a equação 7 para o cálculo final da reputação. Já para a mentira complementar, o efeito do ataque no percentual de decisões acertadas é reduzido, conforme figura 2(b).

A figura 2(c) apresenta uma piora de desempenho para os mecanismos adaptedExponentialAverage e enhancedReputation com o aumento de ζ. Isso ocorre porque com o

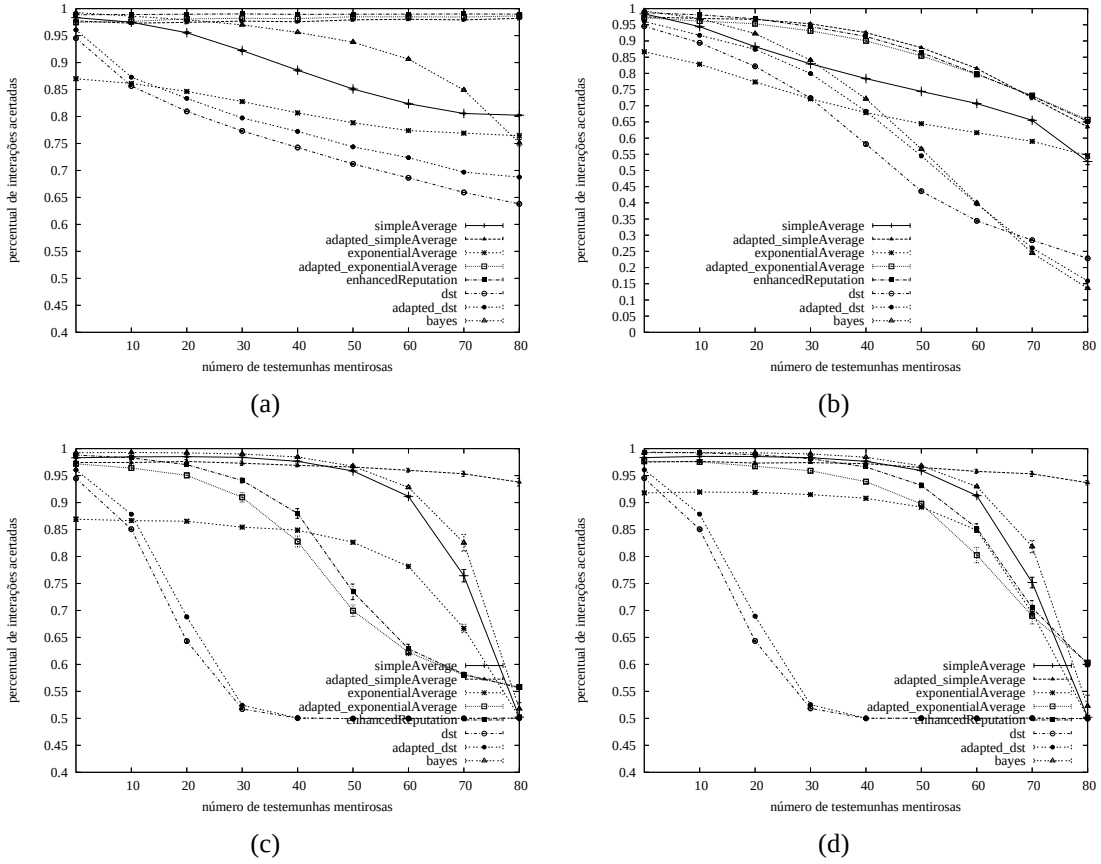

Figura 2. (a)Exagero positivo (c)Mentira Complementar (b)Exagero negativo com fator de decaimento 0.6 (d)Exagero negativo com fator de decaimento 0.5

aumento do peso das informações de primeira mão, os mecanismos exponenciais ficam sujeitos aos efeitos da utilização do fator de decaimento que foram estudados no trabalho [da Silva and de Rezende 2007]. Neste artigo, foi verificado que o maior peso dado às avaliações mais recentes na agregação das informações de primeira mão pode fazer com que poucos erros consecutivos de um provedor bem comportado o faça ser julgado como mau. A figura 2(d) mostra o melhor resultado obtido quando o fator de decaimento adotado é 0.5 no lugar do 0.6.

As simulações foram refeitas considerando $\zeta = 0.5$, mas reduzindo a capacidade do histórico para 10 avaliações. A figura 3(a) mostra uma melhora significativa no desempenho dos métodos dst, adaptedDST e simpleAverage em relação às primeiras simulações. No caso dos métodos que usam dst, a capacidade do histórico tem participação direta no cálculo das crenças de primeira mão através da equação 14. Quanto maior for o histórico, mais lentamente a crença na incerteza $m(T, notT)$ cederá espaço para a crença em alguma hipótese de comportamento do conjunto θ, o que causa demora na identificação de provedores mal comportados. Já para o caso do simpleAverage, a capacidade do histórico tem influência através da equação 6. Quanto menor o histórico, mais cedo estará preenchido e as informações de segunda mão deixarão de ser consideradas. A figura 3(b) confirma a melhora de desempenho dos métodos dst, adaptedDST e simpleAverage.

A figura 3(a) também mostra uma piora no desempenho do método exponen-

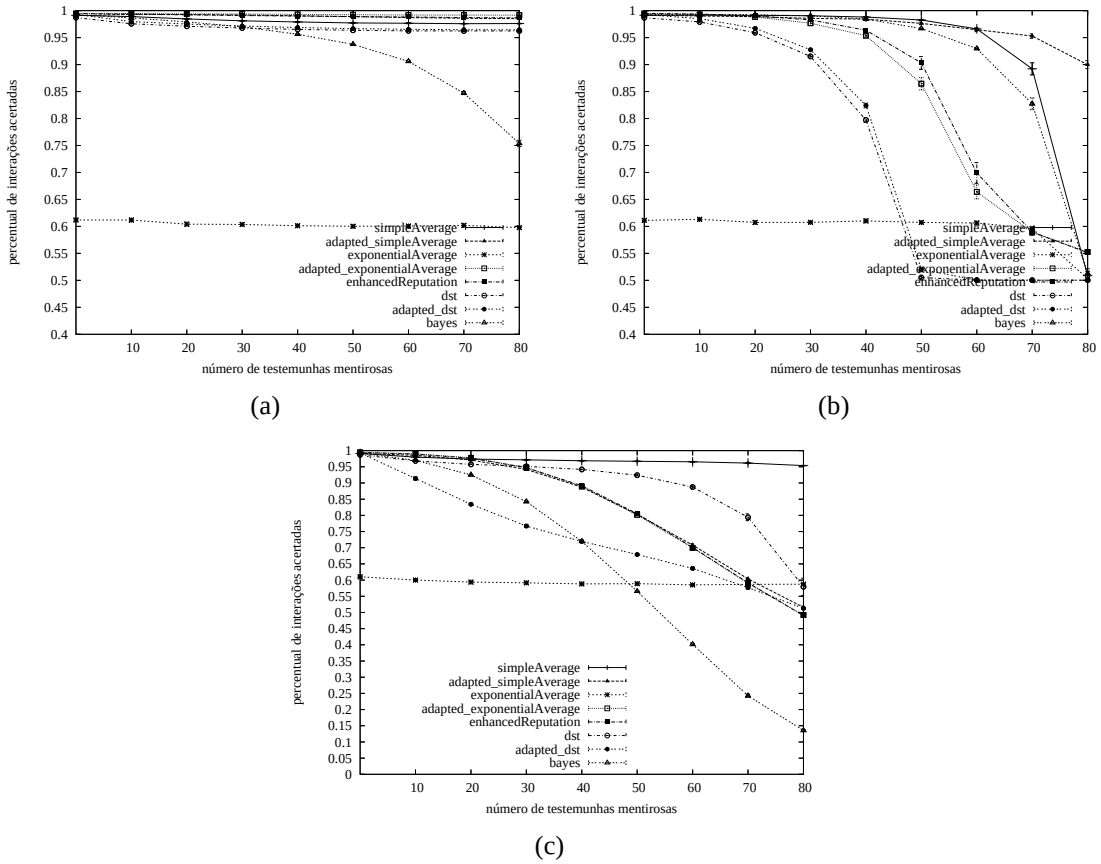

Figura 3. (a)Exagero positivo; (b)Exagero negativo (c)Mentira Complementar

tialAverage. Este método também usa a equação 6 e, com uma capacidade pequena de histórico, ele deixará rapidamente de usar as informações de segunda mão. Entretanto, no caso deste método, isso não é uma vantagem porque, conforme foi visto em [da Silva and de Rezende 2007], um histórico pequeno piora muito o efeito causado pela utilização do fator de decaimento fazendo com que pouquíssimas falhas consecutivas de um provedor bem comportado já sejam suficientes para que ele seja erradamente considerado como mal. Os métodos adaptedExponential e enhancedReputation não sofrem mudança significativa. Ambos continuam usando informações de segunda mão, que amenizam os efeitos da utilização do pequeno histórico e do fator de decaimento.

A figura 3(c) mostra que os efeitos sofridos pelos métodos são análogos quando o modelo matemático da mentira é a mentira complementar. É importante observar ainda que, apesar do método Bayesiano não usar histórico nem a constante ζ no cálculo final da reputação, a inclusão deste método nas simulações permitiu sua comparação com os demais métodos. Foram feitas também simulações considerando $\zeta = 0.6$, mas com a capacidade do histórico configurada para 10 avaliações. Os resultados foram análogos aos anteriores com $\zeta = 0.6$, então não serão incluídos aqui por questão de espaço.

As figuras 4 e 5 mostram como o ataque do conluio influencia cada método. Note que os clientes em conluio não sofrem nenhum tipo de efeito do ataque que praticam porque ao trocarem informações de segunda mão entre si, eles não mentem. Sendo assim, essa é a forma mais vantajosa de praticar o ataque do testemunho mentiroso.

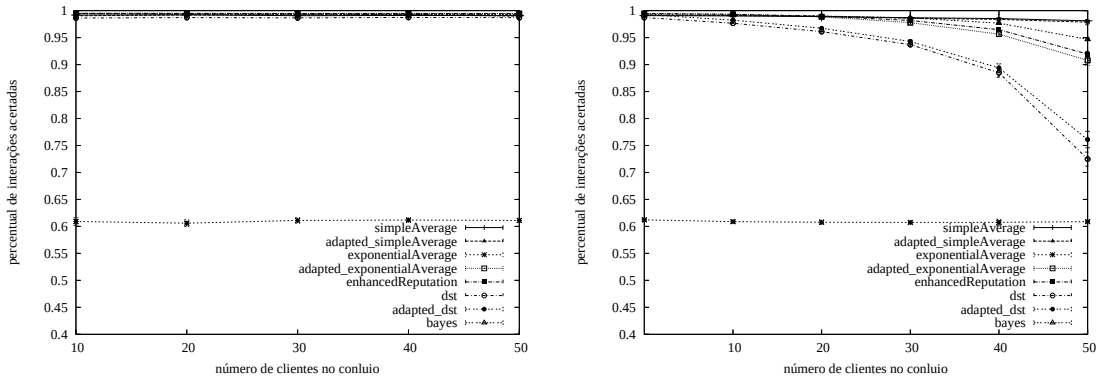

Figura 4. Conluio usando exagero positivo para elogiar e negativo para difamar: (a) Clientes do grupo (c) Clientes vítimas do ataque

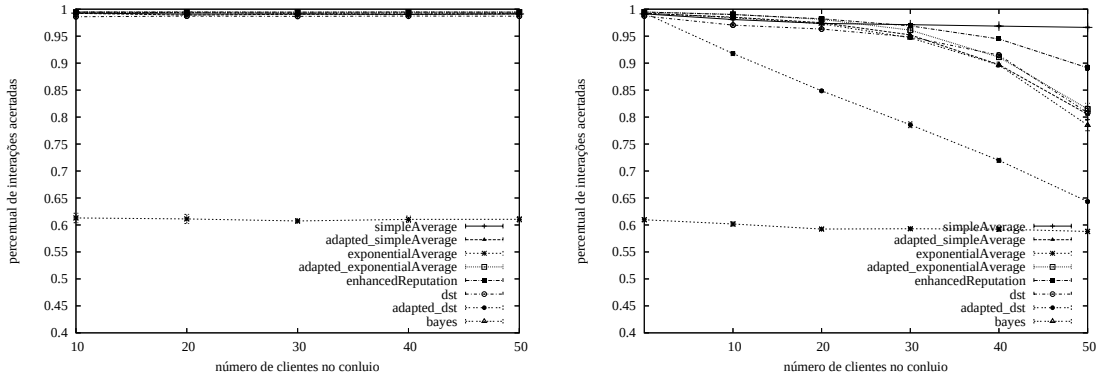

Figura 5. Conluio usando mentira complementar: (a) Clientes do grupo (c) Clientes vítimas do ataque

6. Conclusão e Trabalhos Futuros

No modelo exagero positivo, os métodos funcionam melhor quando usam históricos menores, com exceção do exponentialAverage, que tem um pior desempenho neste caso, e do bayes, que não é afetado por este parâmetro. O mesmo comportamento vale para o exagero negativo, mas este modelo afeta mais os métodos que o anterior. O modelo matemático de mentira que teve maior influência nos métodos foi a mentira complementar. Com relação aos métodos que usam sempre informação de segunda mão, foi constatado que, independente do modelo de mentira usado pelas testemunhas mentirosas, o maior peso associado à informação de primeira mão realmente diminui os efeitos deste ataque. Entretanto, para o caso dos mecanismos de reputação que usam métodos exponenciais, uma atenção especial deve ser dada ao fator de decaimento, que deve ser reduzido. O mecanismo Bayesiano também não é afetado por este parâmetro. Quanto ao conluio, ficou demonstrado que é a maneira mais vantajosa para um *peer* praticar o ataque do testemunho mentiroso, visto que ele não é afetado pelo ataque porque troca informações de segunda mão com os demais participantes do conluio e estes não mentem entre si.

É importante mencionar que, apesar do estudo da robustez dos métodos ao ataque

do testemunho mentiroso ser um importante passo, outros estudos são necessários para embasar os desenvolvedores de aplicações P2P no momento de escolher que mecanismo de reputação é o mais indicado para o ambiente no qual está desenvolvendo. A versão final do simulador está em teste e permitirá gerar cenários diferentes dos apresentados neste trabalho, pois, incluirá um novo modo de operação onde cada cliente gerenciará sua própria lista de provedores ordenada por reputação de forma a se tornar capaz de escolher o provedor com o qual deseja interagir. Além disso, caso não consiga sucesso com o provedor que escolheu, poderá fazer quantas tentativas julgar necessárias dentro de uma mesma interação, requisitando o serviço desejado a outros provedores de sua lista. Também será possível simular os mecanismos de reputação trabalhando em conjunto com mecanismos de credibilidade e comparar os ganhos nas performances dos métodos com relação aos resultados apresentados neste trabalho. Três propostas de mecanismos de credibilidade estão implementadas no simulador, em fase final de depuração.

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.*

da Silva, F. M. and de Rezende, J. F. (2007). Avaliação de métodos matemáticos usados nos modelos de reputação de incentivo à cooperação. In *25º Simpósio Brasileiro de Redes de Computadores (SBRC2007)*.

Hughes, D., Coulson, G., and Walkerdine, J. (2005). Free riding on gnutella revisited: The bell tolls? *IEEE Distributed Systems Online*, 6(6):1.

Liu, J. and Issarny, V. (2004). Enhanced reputation mechanism for mobile ad hoc networks. In *Proceedings of iTrust 2004*, pages 48–62.

Saroiu, S., Gummandi, 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.

Yu, B. and Singh, M. (2002a). Distributed reputation management for eletronic 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*.