COPPE/UFRJ

AVALIAÇÃO DE DESEMPENHO DE MÉTODOS MATEMÁTICOS USADOS NOS MODELOS DE REPUTAÇÃO DE INCENTIVO À COOPERAÇÃO

Fabiana Martins da Silva

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Engenharia Elétrica, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia Elétrica.

Orientador: José Ferreira de Rezende

Rio de Janeiro

Outubro de 2008

AVALIAÇÃO DE DESEMPENHO DE MÉTODOS MATEMÁTICOS USADOS NOS MODELOS DE REPUTAÇÃO DE INCENTIVO À COOPERAÇÃO

Fabiana Martins da Silva

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. José Ferreira de Rezende, D.Sc.

Prof. Aloysio de Castro Pinto Pedroza, D.Sc.

Prof. Dorgival Olavo Guedes Neto, Ph.D.

RIO DE JANEIRO, RJ – BRASIL
OUTUBRO DE 2008

Silva, Fabiana Martins da

Avaliação de Desempenho de Métodos Matemáticos Usados nos Modelos de Reputação de Incentivo à Cooperação/Fabiana Martins da Silva. – Rio de Janeiro: UFRJ/COPPE, 2008.

XIV, 127 p.: il.; 29, 7cm.

Orientador: José Ferreira de Rezende

Dissertação (mestrado) – UFRJ/COPPE/Programa de Engenharia Elétrica, 2008.

Referências Bibliográficas: p. 121 – 127.

1. Modelos de Reputação. 2. Métodos de Incentivo à Coooperação. 3. Cooperação em Peer-to-Peer. I. Rezende, José Ferreira de. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Elétrica. III. Título.

Dedico este trabalho ao amor da minha vida, o meu marido Eduardo Dias Justa Pereira Bastos. A ele agradeço todo amor, carinho, apoio, companheirismo e cumplicidade. Edu, eu te amo do fundo do meu coração!

Agradecimentos

Agradeço a Deus, que me deu saúde, família e amigos maravilhosos e todas as condições que foram necessárias para que eu pudesse finalizar este trabalho.

Aos meus pais, Gilberto e Zuleika; à minha irmã, Flavia; aos meus sogros, Eduardo e Jenifer; à minha cunhada, Mayna; aos meus cunhados, Daniel e Adriano, e a todos da família que compreenderam os períodos em que precisei me ausentar, torcendo e me apoiando ao longo do tempo que dediquei à feitura deste trabalho.

Aos meus grandes amigos Luciano Junqueira, Fabiana Coutinho e Leandro Fernandes, amigos de todas as horas. Aos amigos Marcel, Carlos Henrique, Laila, Yuri e Kleber, do GTA, pelo apoio e contribuições ao longo do mestrado. Aos amigos Alberto, Claudio Sessa, Heitor, Janaina, Jorge Lúcio, Maria Cristina, Marinésio, Sueli e Walter, que trabalham comigo nos Correios, pelo incentivo.

Ao professor José Ferreira de Rezende pela orientação, lutando comigo até o fim.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

AVALIAÇÃO DE DESEMPENHO DE MÉTODOS MATEMÁTICOS USADOS NOS MODELOS DE REPUTAÇÃO DE INCENTIVO À COOPERAÇÃO

Fabiana Martins da Silva

Outubro/2008

Orientador: José Ferreira de Rezende

Programa: Engenharia Elétrica

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, 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.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

PERFORMANCE EVALUATION OF MATHEMATICAL METHODS USED IN REPUTATION MODELS FOR INCENTIVE COOPERATION

Fabiana Martins da Silva

October/2008

Advisor: José Ferreira de Rezende

Department: Electrical Engineering

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 differents 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, Dempster-Shafer Theory. Aspects of convergence, robustness and security of the methods must be well known because theses 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.

Sumário

Referências Bibliográficas **121**

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Motivação

Sistemas *peer-to-peer* (P2P) vêm ganhando bastante importância e atenção nos últimos tempos. Hoje em dia, já são encontradas diversas aplicações P2P e estas contam com um número cada vez maior de usuários. O trabalho [1], por exemplo, afirma que o aplicativo para compartilhamento de arquivos KaZaA [2] tem, em um dia típico, mais de três milhões de usuários ativos compartilhando em torno de 5000 terabytes de conteúdo.

Os sistemas P2P baseiam seu funcionamento em um importante fundamento: a cooperação entre os *peers* da rede. Cada *peer* desempenha tanto o papel de cliente, que requisita e usa serviços ou recursos de servidores, quanto o papel de servidor, que disponibiliza e provê serviços ou recursos a clientes.

Sistemas de compartilhamento de arquivos, de troca instantânea de mensagens e de compartilhamento de ciclos de CPU são exemplos de aplicações P2P. Seja qual for a aplicação, o bom desempenho de uma rede P2P dependerá do comportamento dos *peers* que a constituem. Entretanto, estudos como [3], [4], [5] e [6] demonstraram que boa parte dos usuários não obedece a esta premissa de funcionamento dos sistemas P2P.

Não é incomum a presença dos chamados usuários egoístas (*free riders*). Estes *peers* usam recursos de outros *peers* da rede, entretanto economizam os seus próprios, não os tornando disponíveis ou limitando seu acesso pelos outros *peers*. Exemplos de usuários egoístas são aqueles que disponibilizam o mínimo possível de arquivos e/ou limitam a taxa de *upload* em redes de compartilhamento de arquivos.

O trabalho [4] é um dos que apresenta estatísticas surpreendentes a respeito da

presença de *peers* egoístas em redes P2P. Este artigo apresenta a análise de um *trace* de 24 horas de tráfego do aplicativo Gnutella v0.4 capturado durante o mês de agosto de 2000. O resultado mostra que quase 70% dos usuários não compartilhavam nenhum arquivo e que quase 50% de todas as respostas eram geradas por apenas 1% dos *peers* da rede. O artigo [6] realiza novas medições na versão 0.6 do Gnutella e descreve resultados semelhantes.

Além dos usuários egoístas, também podem estar presentes os maliciosos. Estes prejudicam a rede, não para o benefício próprio como, por exemplo, para economizar recursos, mas apenas para prejudicar outros usuários. Como exemplo de atitude maliciosa é possível citar a disponibilização de arquivos infectados, corrompidos ou de conteúdo falso em uma rede de compartilhamento de arquivos.

A busca pela solução deste problema de mau comportamento dos *peers* de sistemas P2P levou ao desenvolvimento de diversas propostas de mecanismos de incentivo à cooperação. A idéia destes mecanismos é fornecer a cada *peer* da rede a capacidade de diferenciar os *peers* que possuem um bom comportamento daqueles que agem de forma egoísta ou maliciosa.

Um dado *peer* que deseja requisitar um serviço ou recurso poderá fazê-lo a um *peer* bem comportado aumentando muito suas chances de sucesso. Além disso, os mecanismos de incentivo propõem que usuários egoístas e/ou maliciosos sejam punidos. Ao ser detectado pelos *peers* da rede, um usuário mal comportado não deve ser mais atendido e, desta forma, cada *peer* será forçado a cooperar para fazer parte da rede.

Uma das principais linhas de pesquisas nesta área explora o uso de reputação para o desenvolvimento de mecanismos de incentivo. A idéia chave destas propostas 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.

Existem diversas propostas de mecanismos de incentivo baseados em reputação e uma variedade de métodos matemáticos usados para o cálculo da reputação [7], [8], [9], [10], [11], [12], [13]. Algumas soluções usam métodos mais simples como, por exemplo, uma média [13]. Outras optam por métodos mais complexos, como a Teoria de Dempster-Shafer [11], [12].

A adoção de mecanismos de incentivo baseados em reputação para contornar o problema de mau comportamento dos *peers* das redes P2P, entretanto, necessita de um melhor entendimento dos métodos usados para o cálculo da reputação. Aspectos de convergência, robustez e segurança devem ser conhecidos e comparados porque são extremamente importantes no momento de decidir ou não pela implantação de um dado método.

Possibilitar o conhecimento mais profundo dos métodos de cálculo de reputação e, principalmente, prover condições de efetuar comparações justas, colocando-os em condições iguais de testes e avaliando-os segundo os mesmos critérios e métricas é a principal motivação deste trabalho.

1.2 Objetivos

Conforme citado na seção 1.1, existe uma variedade de métodos matemáticos de cálculo de reputação. Entretanto, o desempenho de cada um destes mecanismos é comprovado através de simulações em diferentes cenários, critérios e métricas, que são escolhidos pelos autores de cada uma das propostas. Este trabalho tem como objetivos:

- Propor um conjunto de cenários, critérios e métricas para testes;
- Testar mecanismos de incentivo utilizando diferentes modelos matemáticos de reputação;
- Comparar os desempenhos obtidos pelos mecanismos nos cenários considerados.

Para alcançar estes objetivos, foi desenvolvido um simulador, em linguagem C, capaz de gerar diferentes cenários onde os mecanismos podem ser testados. Os possíveis ambientes de testes serão detalhados no capítulo 4 e poderão contar com *peers* mal comportados; *peers* que mudam de comportamento no meio da simulação; *peers* que atacam o mecanismo de reputação, etc.

Além disso, o simulador ainda pode ser configurado de maneira a permitir que os mecanismos de reputação sejam testados em conjunto com um mecanismo de credibilidade. Este último é um mecanismo adicional que tem o objetivo de proteger o mecanismo de reputação em cenários onde existam *peers* praticando o ataque do testemunho mentiroso.

Foram escolhidas cinco propostas de mecanimos de reputação da literatura para serem testadas no simulador. Cada uma usa um modelo matemático de cálculo de reputação

diferente. Além disso, adaptações de três destas propostas foram implementadas, o que fornece um total de oito mecanismos simulados na ferramenta desenvolvida.

1.3 Organização da Dissertação

Esta dissertação apresenta a análise e a comparação dos resultados obtidos a partir das simulações de oito mecanismos de incentivo à cooperação. No capítulo 2 são apresentados os conceitos básicos de rede *peer-to-peer*, suas mais conhecidas aplicações, as principais arquiteturas existentes e ainda são introduzidos os conceitos básicos de mecanismos de incentivo à cooperação.

O capítulo 3 apresenta conceitos mais aprofundados a respeito dos mecanismos de incentivo à cooperação baseados em reputação, descreve os modelos matemáticos de cálculo de reputação que foram testados, apresenta o ataque do testemunho mentiroso e o ataque da mudança repentina de comportamento e descreve dois mecanismos de credibilidade, que também foram implementados e testados no simulador.

O capítulo 4 detalha as configurações e modos de funcionamento do simulador, os cenários que podem ser gerados através desta ferramenta de simulação e as métricas consideradas para a comparação de desempenho dos mecanismos. Por fim, o capítulo 5 apresenta a análise dos resultados obtidos e o capítulo 6 apresenta as considerações finais e os trabalhos futuros.

Capítulo 2

Conceitos Básicos

Este capítulo apresenta uma visão geral a respeito das redes P2P. A primeira seção descreve as principais características destas redes. As seções seguintes apresentam as mais conhecidas aplicações P2P para compartilhamento de recursos e serviços e as arquiteturas P2P pura, híbrida e estruturada. A última seção apresenta os conceitos básicos dos mecanismos de incentivo à cooperação e descreve duas importantes linhas de pesquisa nesta área.

2.1 Redes Peer-to-Peer

Para entender o interesse pelo desenvolvimento de aplicações para redes P2P e o impressionante número de usuários atualmente fazendo parte destas redes, é essencial compreender os aspectos básicos do funcionamento desta tecnologia. O trabalho [14] enumera os requisitos que devem ser suportados pelas redes P2P. Dentre eles destacam-se:

- Nós podem estar localizados nas bordas da rede;
- Nós podem possuir diferentes taxas de transmissão;
- Nós podem possuir conectividade variável ou temporária e endereços variáveis;
- Nós devem ser capazes de fornecer e consumir recursos ou serviços de outros nós;
- Nós comunicam-se diretamente uns com os outros.

O primeiro requisito deixa claro que usuários comuns, não apenas os detentores de *hardware* de alto desempenho, podem fazer parte de uma rede P2P. O segundo e o terceiro

requisitos ressaltam que a conexão do usuário pode ser dos mais diversos tipos (discada, banda larga, etc.) e, além disso, o usuário tem a liberdade de se conectar e desconectar da rede quando achar conveniente.

Os dois últimos requisitos citados referem-se ao modelo de comunicação seguido pelos nós deste tipo de rede. Diferente do modelo Cliente/Servidor, caracterizado pela figura de um nó servidor central oferecendo serviços ou recursos a nós clientes, os sistemas P2P baseiam seu funcionamento em um importante fundamento: a cooperação entre os *peers* da rede. Cada *peer* desempenha tanto o papel de cliente, quanto o papel de servidor. Alguns autores até se referem aos *peers* como *servents*, união das palavras *server* e *client* que, traduzidas do inglês, significam servidor e cliente, respectivamente.

2.2 Aplicações Peer-to-Peer

Aplicações P2P têm sido desenvolvidas e utilizadas para o compartilhamento dos mais variados tipos de recursos e serviços. Esta seção apresenta duas aplicações P2P conhecidas: os sistemas de compartilhamento de arquivos e os sistemas de troca instantânea de mensagens.

2.2.1 Troca Instantânea de Mensagens

A troca instantânea de mensagens é uma área de aplicação das redes P2P que vem sendo bastante difundida, principalmente com o aumento do número de usuários que acessam a Internet através de conexão banda larga. ICQ [15], MSN [16] e Yahoo! Messenger [17] são exemplos de aplicativos para troca instantânea de mensagens.

Além do serviço de troca de mensagens em tempo real, alguns destes aplicativos oferecem outras funcionalidades como, transferência de arquivo, *Voice/Vídeo Chat*, etc. Da mesma maneira como as funcionalidades oferecidas variam de um aplicativo para o outro, existem algumas diferenças nas arquiteturas usadas nestes sistemas [18], [19].

Na maioria dos casos, o usuário efetua o *download* e a instalação de um aplicativo de troca instantânea de mensagens que o possibilitará fazer parte desta rede P2P quando ele desejar. Quando o usuário decidir efetuar seu *login* na rede, seu aplicativo se conectará a um servidor que, na realidade, é um nó dedicado que tem uma função de controle na rede. Ele é o responsável por enviar, ao *peer* que está efetuando *login*, informações a respeito

dos integrantes de sua lista de contatos. Além disso, deverá enviar, a cada integrante desta lista de contatos, informações deste *peer* que acaba de se conectar.

Apesar desta fase de *login* seguir, geralmente, o modelo Cliente/Servidor, dois usuários que iniciarem uma comunicação poderão trocar mensagens através de uma conexão direta, ou seja, *peer-to-peer*. Um exemplo que segue este modelo é o ICQ. Em outros casos, até mesmo a troca de mensagens é intermediada pelo servidor, como é o caso do MSN e do Yahoo! Messenger. Nestes sistemas, a comunicação *peer-to-peer* é usada para outras funcionalidades como, por exemplo, para transferência de arquivos, webcam, etc.

Essa arquitetura de redes P2P que, além dos *peers* exercendo simultaneamente papéis de cliente e servidor, admite a presença de nós dedicados exercendo funções de controle é chamada de arquitetura P2P híbrida, como será visto na seção 2.3.2.

2.2.2 Compartilhamento de Arquivos

As aplicações P2P para compartilhamento de arquivos são muito populares e intensamente estudadas, existindo uma vasta gama de trabalhos publicados nesta área. Os artigos [3], [4], [5], [6], [20], [21], [22], [23], [24] e [25] são exemplos de pesquisas desenvolvidas com este enfoque. Napster [26], Gnutella [27], FreeNet [28] e KaZaA [2] são exemplos de aplicativos.

Os mais diversos tipos de arquivos podem ser trocados entre os *peers* como, por exemplo, arquivos de áudio, vídeo, texto, executáveis, etc. Nestas aplicações, cada usuário constitui um *peer* capaz de identificar outros *peers* da rede que estão disponibilizando os arquivos de interesse. Uma vez encontradas as possíveis fontes dos arquivos desejados, será importante então a escolha daquelas a partir das quais *downloads* serão feitos.

Assim como acontece com as aplicações de troca instantânea de mensagens, existem diferentes arquiteturas usadas pelos sistemas de compartilhamento de arquivos. No caso destes sitemas, o mecanismo de busca por *peers* disponibilizando arquivos de interesse irá variar de acordo com a arquitetura adotada. Dada a enorme popularidade dos aplicativos de compartilhamento de arquivos e a grande quantidade de estudos desenvolvidos nesta área, uma discussão detalhada a esse respeito será dada na seção 2.3, que tratará das arquiteturas dos sistemas P2P.

2.3 Arquiteturas Peer-to-Peer

A descrição das redes P2P como sendo redes constituídas por *peers* que exercem simultaneamente os papéis de cliente e servidor dá a impressão de que todos os nós têm a mesma função dentro da rede e que não pode haver hierarquia como existe no modelo Cliente/Servidor. De fato, esta é uma arquitetura possível, adotada inclusive pela versão 0.4 do aplicativo Gnutella, mas é importante entender que não é a única arquitetura existente.

É admissível, também em redes P2P, a presença de nós servidores atuando em um nível hierarquicamente acima dos demais *peers* e exercendo funções de controle. Nesta seção, as principais arquiteturas, usadas pelas mais conhecidas aplicações P2P serão descritas. Mais informações podem ser encontradas em [3], [4], [6], [14], [20], [21] e [24], [29] e [30].

2.3.1 Arquitetura P2P Pura

Na arquitetura P2P conhecida como "pura", não existe hierarquia e todos os nós que constituem a rede têm a mesma funcionalidade: compartilhar serviços ou recursos com os demais nós da rede. Exemplos de aplicações que adotam esta arquitetura são os aplicativos para compartilhamento de arquivos Gnutella v0.4 e FreeNet.

Em um sistema P2P de compartilhamento de arquivos que adota arquitetura P2P pura, a busca por provedores é efetuada através de uma "inundação controlada". Um *peer* interessado em um dado arquivo envia uma mensagem de consulta (*Query Message*) para cada um dos seus vizinhos. Cada *peer* que receber esta mensagem deve verificar se possui o arquivo que está sendo procurado e, em caso positivo, gerar uma mensagem de resposta em direção ao *peer* que originou a consulta. Além disso, deverá também repassar a consulta para seus próprios vizinhos (menos para aquele de quem recebeu a mensagem).

Desta maneira, um *peer* em busca de um arquivo irá inundar a rede com sua consulta e essa inundação será controlada apenas pelo valor do campo TTL (*Time To Live*) da mensagem. Esse campo será então o responsável por definir o alcance da consulta. O *peer* que originou a consulta usará as respostas recebidas para escolher um provedor a quem enviará diretamente uma mensagem requisitando o arquivo desejado.

2.3.2 Arquitetura P2P Híbrida

A arquitetura P2P "híbrida" recebe este nome porque possui características tanto da arquitetura Cliente/Servidor quanto da arquitetura P2P pura. Os *peers* que se integram a estas redes exercem simultaneamente os papéis de cliente e servidor, entretanto, nem todo trabalho necessário ao funcionamento do sistema é executado pelos usuários de forma descentralizada. Alguns nós especiais centralizam funções de controle.

Na seção 2.2.1 foi mencionado que aplicativos P2P de troca instantânea de mensagens, como ICQ, adotam arquitetura híbrida. Outro exemplo é o Napster, para compartilhamento de arquivos, cuja função centralizada é a busca, executada por nós dedicados conhecidos como "servidores de índices". Cada um destes servidores tem a função de catalogar os arquivos que estão sendo disponibilizados por cada *peer* conectado a ele.

Ao efetuar *login* na rede, cada *peer* se conecta a um servidor de índices e o envia uma lista de todos os arquivos que pretende disponibilizar. Quando um *peer* deseja buscar por um arquivo de interesse, envia sua consulta ao servidor de índices ao qual está conectado. O servidor fará uma busca nas informações que armazena e retornará os possíveis provedores. Terminada a fase de busca, a fase de *download* é feita sem a participação de nenhum servidor, exatamente como na arquitetura P2P pura.

Para que a função de busca continue funcional nestas redes, os servidores de índices devem estar sempre atualizados. Quando um *peer* da rede terminar um *download*, ele deve informar ao servidor ao qual está conectado sobre o novo arquivo que está disponibilizando. O servidor também deve ser informado caso o *peer* deixe de disponibilizar algum arquivo.

O trabalho [20] mostra outras soluções de busca que podem ser adotados em sistemas P2P de arquitetura híbrida.

2.3.3 Arquitetura P2P Estruturada

A arquitetura P2P estruturada usa DHT (*Distributed Hash Table* - Tabela Hash Distribuída). Neste modelo, o documento compartilhado recebe um identificador que é o resultado de uma *hash* de seu nome e conteúdo.

Cada *peer* encaminha o documento a ser compartilhado para o *peer* cujo ID é o mais próximo do identificador deste documento. Até que o documento atinja este *peer* destino, cada *peer* que o recebe e repassa também guarda uma cópia sua.

Com relação à busca, também é feita através do identificador do documento desejado. O *peer* que deseja um documento, enviará sua requisição em direção ao *peer* cujo ID se aproxima mais do identificador do documento. A busca terminará quando uma cópia do documento desejado for encontrada.

Os artigos [14] e [29] apresentam diferentes algorítmos que implementam esta arquitetura como, por exemplo, Chord, CAN, dentre outros.

2.4 Mecanismos de Incentivo à Cooperação

Como foi dito anteriormente, estudos como [3], [4], [5] e [6] demonstraram que muitos usuários de sistemas P2P apresentam comportamento não colaborativo. Sendo a cooperação entre os *peers* uma premissa de funcionamento destes sistemas, torna-se importantíssima à implementação de algum mecanismo que incentive os *peers* a cooperar.

Para melhor entender essa necessidade, basta observar o exemplo das tão conhecidas redes P2P de compartilhamento de arquivos. Nesses sistemas, um *peer* que efetua o *download* de um arquivo deveria, idealmente, se tornar provedor do mesmo. Assim sendo, cópias deste arquivo seriam distribuídas pela rede e, quanto maior fosse a sua popularidade, maior seria o número de *peers* adquirindo-o e tornando-se capaz de fornecê-lo.

A disseminação de arquivos compartilhados ajuda no aumento da escalabilidade e do sistema, pois evita a concentração das requisições num servidor central ou num conjunto pequeno de servidores. A cooperação também traz as vantagens da redundância, fazendo com que vários *peers* sejam capazes de fornecer o recurso compartilhado. Se existe uma grande quantidade de *peers* mal comportados, o trabalho dos *peers* com comportamento colaborativo é prejudicado porque eles passam a ser mais requisitados do que deveriam e podem até ser sobrecarregados. Um usuário colaborativo que se sinta prejudicado ou sobrecarregado por adotar tal postura, tenderá a de se tornar mais um egoísta, piorando o desempenho da rede.

Para combater o mau comportamento dos *peers* em sistemas de compartilhamento de arquivos bem como em qualquer outro sistema P2P, inúmeras propostas de mecanismos de incentivo à cooperação foram feitas. Mecanismos de incentivo baseados em créditos e mecanismos de incentivo baseados em reputação são as duas principais linhas de pesquisa exploradas.

2.4.1 Mecanismos de Incentivo Baseados em Crédito

A idéia principal explorada pelas soluções baseadas em créditos é que um dado *peer* deve pagar pelos serviços/recursos requisitados a outros *peers* e cobrar pelos serviços/recursos fornecidos a outros *peers*. Desta maneira, os *peers* serão obrigados a colaborar, pois essa será a forma de acumular créditos para pagar pelos serviços/recursos desejados.

Além da sua aplicação em redes P2P [31] e [32], os mecanismos baseados em créditos já foram estudados para outras aplicações. Em [33], [34] e [35], por exemplo, foram explorados com o objetivo de aumentar o desempenho de redes *ad hoc* na presença de nós mal comportados.

A ausência de infra-estrutura das redes *ad hoc* faz com que o roteamento de mensagens se torne dependente da colaboração dos nós que as constituem. Se os nós da rede pertencem a uma mesma administração, então é esperado que eles colaborem entre si. Entretanto, no caso de pertencerem a diferentes administrações, não há garantias que um nó da rede esteja disposto a colaborar repassando as mensagens de seus vizinhos já que, fazendo isso, estaria gastando energia com o roteamento de mensagens que não são de seu interesse. Trabalhos como [36], [37] e [38] estudam a necessidade de um mecanismo de incentivo para esses casos.

2.4.2 Mecanismos de Incentivo Baseados em Reputação

Como foi dito anteriormente, a idéia dos mecanismos baseados em reputação 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.

Tendo em vista que os mecanismos de incentivo à cooperação baseados em reputação são o foco de estudo deste trabalho, o capítulo 3 descreverá os detalhes de funcionamento destes mecanismos, suas diferentes arquiteturas, importantes diferenças existentes entre algumas propostas, aspectos de segurança, dentre outros assuntos relacionados.

Capítulo 3

Incentivo à Cooperação Usando Reputação

Este capítulo apresenta importantes conceitos a respeito dos mecanismos de incentivo à cooperação baseados em reputação. A primeira seção descreve as arquiteturas centralizada e descentralizada que podem ser adotadas por estes mecanismos. A seção seguinte discute sobre a importância da escolha dos critérios e métricas de avaliação de comportamento e como este assunto é tratado na literatura. Posteriormente, uma seção trata das diversas nomeclaturas usadas na literatura e apresenta aquela que será adotada ao longo desta dissertação.

Uma seção é dedicada à apresentação dos oito métodos matemáticos de cálculo de reputação que foram considerados nas simulações desta dissertação. A seção seguinte discute como cada mecanismo estudado usa o valor calculado de reputação no julgamento do comportamento dos provedores. Em seguida, dois conhecidos ataques aos mecanismos de reputação são apresentados, o ataque da mudança repentina de comportamento e o ataque do testemunho mentiroso. Na última seção, são descritos os princípios de funcionamento dos mecanismos de credibilidade e dois mecanismos, simulados neste trabalho em conjunto com os mecanismos de reputação, são apresentados.

3.1 Arquiteturas dos Mecanismos Baseados em Reputação

Esta seção apresenta os principais conceitos e diferenças entre as arquiteturas centralizada e descentralizada de mecanismos de incentivo baseados em reputação.

3.1.1 Mecanismos Centralizados

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. Ao final de uma interação, o *peer* que requisitou algum serviço/recurso avalia o *peer* com o qual interagiu e envia esta avaliação à entidade responsável pelas reputações. Esta entidade atualizará a reputação associada a este *peer* através de algum método matemático de cálculo de reputação. Quando um *peer* desejar se informar a respeito da reputação de outro, deverá requisitar esta informação à entidade central responsável pelas reputações.

Um dos mais citados exemplos de aplicações que usam mecanismos de incentivo baseados em reputação com arquitetura centralizada é o site eBay [39]. Trata-se de um site voltado para o comércio eletrônico e usado por pessoas físicas ou empresas para comercializar produtos e serviços. Segundo a descrição dada pelo próprio site eBay a respeito do funcionamento de seu sistema de reputação, após cada transação efetuada, o vendedor e o comprador podem executar avaliações mútuas. Esta avaliação consiste na escolha de uma das três possíveis notas - positiva, negativa ou neutra.

O cálculo da reputação de cada participante é feito então através da soma das avaliações positivas (informadas por diferentes participantes) menos a soma das avaliações negativas que ele recebeu (informadas por diferentes participantes). Avaliações neutras não impactam o valor da reputação de nenhuma maneira. Além de informar a avaliação dada ao membro com o qual interagiu, cada participante da rede pode também enviar ao site eBay um comentário dando mais detalhes a respeito da transação efetuada.

O trabalho [40] descreve inúmeras outras aplicações que implementam mecanismos de incentivo baseados em reputação com arquitetura centralizada.

3.1.2 Mecanismos Descentralizados

Na arquitetura descentralizada, não existe uma entidade central para calcular, atualizar e publicar a reputação dos *peers* da rede, ou seja, quando um *peer* deseja conhecer a reputação de outro, não há a quem ele possa requisitar esta informação. Sendo assim, o trabalho de calcular e manter atualizada a medida de reputação de cada *peer* será executado localmente por cada *peer* da rede.

Ao término de uma interação, o *peer* que requisitou algum serviço/recurso avalia o *peer* com o qual interagiu. O resultado desta avaliação é armazenado pelo *peer* que a efetuou. Cada *peer* da rede mantém históricos de avaliações geradas a partir de suas experiências com outros *peers*. Estas informações armazenadas são usualmente conhecidas por "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 *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, torna-se importante que cada *peer* não conte somente com as informações que armazena localmente.

Nos mecanismos de incentivo com arquitetura descentralizada, os *peers* trocam experiências entre si. As informações recebidas de outros *peers*, geradas a partir das interações das quais eles participaram, são comumente chamadas de informações de segunda mão.

Mecanismos de incentivo à cooperação baseados em reputação de arquitetura descentralizada têm sido intensamente estudados para aplicação em redes *ad hoc* [7], [41], [42], [43], [44], [45] e [46]. Como foi citado na seção 2.4.1, nestas redes não existe infraestrutura e o roteamento de pacotes é feito pelos próprios nós. Com a aplicação de um mecanismo de incentivo baseado em reputação, um nó poderia analisar a reputação de seus vizinhos no momento de escolher a quem requisitar o repasse de suas mensagens.

O maior interesse deste trabalho, entretanto, está voltado para outra área de aplicação: As redes P2P. Os trabalhos [8], [9], [10], [11], [12], [13], [47] [48] e [49] são exemplos de propostas que podem ser aplicadas no ambiente P2P. Maiores detalhes da aplicação de mecanismos de reputação em redes P2P serão dados ao longo deste trabalho.

3.2 Critérios e Métricas de Avaliação de Comportamento

Independente da arquitetura adotada, qualquer mecanismo de incentivo baseado em reputação tem, como etapa essencial ao seu funcionamento, as avaliações que cada *peer* realiza de cada um dos *peers* com os quais interage. Os métodos de avaliação podem ser caracterizados por duas importantes questões:

- O que é observado durante a interação?
- Como é feito o mapeamento do que é observado em valores que possam ser manipulados matematicamente?

O primeiro questionamento se refere ao critério de avaliação, ou seja, que aspectos do comportamento de um *peer* são observados no momento de efetuar sua avaliação. Se o critério a ser usado por cada *peer* não é definido, ou seja, diferentes *peers* adotam diferentes critérios, o cálculo da reputação pode ser prejudicado e todo o mecanismo de incentivo à cooperação comprometido.

Como exemplo, no site eBay (descrito na seção 3.1.1), alguns compradores podem dar uma avaliação negativa a um vendedor por causa do tempo de entrega enquanto que outros podem avaliá-lo positivamente por causa da qualidade do produto. Como o cálculo da reputação considera as avaliações indiscriminadamente, um comprador não poderá ter uma noção precisa do comportamento deste vendedor apenas observando seu valor de reputação no site. Será necessário ler os comentários deixados pelos participantes que já interagiram com ele para interpretar melhor o valor de reputação, observando as reclamações e elogios e os aspectos que foram considerados em cada depoimento.

Outro exemplo pode ser um *peer*, participante de uma rede P2P de compartilhamento de arquivos, que adota como critério de avaliação a qualidade dos arquivos e recebe informações de segunda mão geradas a partir de avaliações que consideraram velocidade de *download*. Neste caso, o mau comportamento indicado pelas informações de segunda mão a respeito de um provedor com baixa velocidade pode influenciar no cálculo da reputação levando o *peer* cliente à decisão de não interagir, ainda que este provedor possa fornecê-lo arquivos de qualidade.

Apesar da importância da adoção de um mesmo critério de avaliação por todos os participantes da rede, diversas propostas não discutem este assunto [8], [11], [12] e [13]. Outras citam que as reputações calculadas pelos *peers* devem estar associadas a um mesmo

aspecto de comportamento observado durante a interação [50]. De uma maneira geral, os trabalhos procuram não especificar quais devem ser estes aspectos, pois é interessante que esta escolha fique a cargo dos desenvolvedores de aplicações.

Na maioria dos mecanismos de reputação propostos, se mais de um aspecto são analisados durante cada interação, os *peers* calcularão, para cada outro participante da rede, um valor de reputação por aspecto. Já os trabalhos [9] e [10] argumentam que, além dos valores de reputação por aspecto, pode ser interessante oferecer a possibilidade de calcular valores de reputação associados a um grupo de aspectos. Estes dois trabalhos apresentam o uso de um método Bayesiano para possibilitar este cálculo.

Com relação às simulações executadas nesta dissertação, tendo em vista que o foco é o estudo dos modelos matemáticos de cálculo da reputação descritos no item 3.4, e não os critérios de avaliação existentes, assume-se que todos os *peers* que constituem a rede usam um só critério de avaliação, comum a todos os participantes da rede. Entretanto, nada impede que os métodos estudados sejam usados em redes onde seja necessária a análise de diversos aspectos. Nestes casos, pode-se considerar que será gerado um valor de reputação por aspecto, ou se utilizará algum artifício matemático para agrupar as avaliações dadas aos diferentes aspectos.

Como foi dito no início desta seção, além da escolha dos aspectos que serão observados durante a avaliação, outra importante característica dos métodos de avaliação é a maneira usada para representar numericamente o que é avaliado. O site eBay possibilita que seus usuários avaliem escolhendo um entre os três possíveis valores de avaliação: Positivo, neutro ou negativo. Já nos artigos [8], [9] e [10], a representação das avaliações é binária, ou seja, valor 0 para julgar o comportamento como insatisfatório e valor 1 para julgar como satisfatório.

No trabalho [7], cada avaliação é feita através da escolha de um valor dentro do intervalo [-1, 1]. Quanto mais próxima de -1 for a avaliação de um *peer*, mais insatisfatório foi considerado seu comportamento. De maneira análoga, quanto mais próximo de 1 for a avaliação, mais satisfatório o comportamento foi considerado. Já os trabalhos [11], [12], e [13] são exemplos que adotam o intervalo de valores [0,1]. Avaliações próximas de 0 expressam insatisfação enquanto que aquelas próximas de 1 caracterizam satisfação.

3.3 As Várias Definições para Reputação e Confiança

Nesta seção, a diversidade de definições para os termos reputação (*reputation*) e confiança (*trust*) é debatida. Esta diferença conceitual existente entre as propostas pode atrapalhar o entendimento dos mecanismos e dificultar a comparação entre eles. O objetivo desta seção é esclarecer algumas destas diversas definições e nomenclaturas existentes, oferecendo o embasamento necessário para concluir as definições e nomenclaturas que serão adotadas nesta dissertação.

Os trabalhos [44] e [8] definem reputação como sendo a performance de um nó da rede, observada por outros nós. Esta performance é a maneira como um dado nó executa uma tarefa, que pode ser o repasse de mensagens em uma rede *ad hoc*, o compartilhamento de arquivos em uma rede P2P, etc. Nestes trabalhos confiança é o termo usado para se referir à medida de honestidade do nó nos momentos de oferecerem informações de segunda mão (maiores detalhes deste assunto na seção 3.6.1).

O artigo [42] define reputação como a medida da confiança inspirada por um participante da rede dentro de um contexto. O artigo chama de *subjective reputation* a reputação baseada em informações de primeira mão. *Indirect reputation* é descrita como sendo a reputação calculada a partir das informações de segunda mão. Já *funcional reputation* é o nome dado à reputação calculada a partir da agregação de *subjective reputations* e *indirect reputations* associadas a diferentes aspectos de avaliação.

O problema da diversidade de definições que existe para os termos reputação e confiança também é discutido por [7]. Este trabalho define confiança em um dado nó como sendo uma previsão de suas futuras ações. O artigo quer dizer que um nó confiável é aquele com o qual uma interação tem grande probabilidade de ser bem sucedida. Um importante fator que afeta esta previsão é justamente a reputação. Quanto maior o valor da reputação de um nó, maior é a confiança neste nó. Em [7], o cálculo do valor da reputação é baseado em informações de primeira e segunda mão.

Já os trabalhos [9] e [10] definem confiança como sendo uma crença baseada nas informações de primeira mão, enquanto que reputação é uma crença baseada em informações de segunda mão.

As definições de reputação e confiança adotadas nesta dissertação serão similares às do artigo [7]. Reputação é um valor numérico, calculado a partir da combinação de informações de primeira e segunda mão. A confiança que um nó possui em outro pode

ou não estar associada à reputação, ou seja, um nó pode confiar em outro porque observou que seu valor de reputação é alto, ou simplesmente porque, por exemplo, são nós conhecidos, que têm alguma relação ou contrato. Além destas definições de reputação e confiança, adota-se o termo credibilidade para a medida de honestidade dos *peers* nos momentos de oferecerem informações de segunda mão.

3.4 Métodos Matemáticos para o Cálculo da Reputação

Esta seção apresenta os oito métodos matemáticos de cálculo de reputação que foram comparados a partir das simulações executadas por este trabalho.

3.4.1 Média Simples (*simpleAverage*)

O uso de média simples é uma opção de baixa complexidade para calcular a reputação. Considerando a proposta apresentada em [13], 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:

$$R(P_i, P_j) = \begin{cases} \sum_{k=1}^{h} e_{ij}^{k} / \ h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases} \tag{3.1}$$

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:

$$T(P_i, P_j) = \begin{cases} \sum_{k=1}^{L} w_k * R(W_k, P_j) / \ L & \text{if } L \neq 0; \\ 0.5 & \text{if } L = 0. \end{cases} \tag{3.2}$$

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

Como será visto na seção 3.6.1, um dos ataques muito comuns a mecanismos de reputação é o ataque do testemunho mentiroso. Um *peer* praticando este ataque, ao receber requisições de informações a respeito de um provedor, informa uma reputação diferente da que calculou a partir de suas experiências com este provedor. A maioria das propostas de mecanismos de reputação 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. A seção 3.7 fornecerá uma descrição mais detalhada destes mecanismos.

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

$$Rep(P_i, P_j) = \eta * R(P_i, P_j) + (1 - \eta) * T(P_i, P_j) \tag{3.3}$$

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.

3.4.2 Média Simples Adaptada (*adapted_simpleAverage*)

A seção 3.4.1 descreveu um método de cálculo de reputação que usa média simples. Como foi mostrado, este método só usa informações de segunda mão enquanto os históricos não estiverem cheios. Nesta seção, apresenta-se uma pequena adaptação, que resultará num novo método cujo comportamento será estudado durante as simulações. O método adaptado de média simples sempre utiliza a informação de segunda mão no cálculo do valor final de reputação.

Sendo assim, as informações de primeira mão serão agregadas pela equação 3.1 e as informações de segunda mão serão agregadas pela equação 3.2. A adaptação proposta será no cálculo final de reputação. Um *peer* cliente P_i calculará o valor final de reputação para um *peer* provedor P_j através da seguinte equação:

$$Rep(P_i, P_j) = \alpha * R(P_i, P_j) + (1 - \alpha) * T(P_i, P_j) \tag{3.4}$$

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

3.4.3 Média Exponencial (*exponentialAverage*)

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.

A proposta de [13], usa a seguinte função para agregar informações de primeira mão:

$$R(P_i, P_j) = \begin{cases} (1-\gamma)^{(h-1)} * e_{ij}^1 + (1-\gamma)^{(h-2)} * \gamma * e_{ij}^2 + ... + (1-\gamma)^0 * \gamma * e_{ij}^h & \text{if } h \neq 0; \\ 0 & \text{if } h = 0. \end{cases} \tag{3.5}$$

onde γ, variável chamada comumente de fator de decaimento (*fading factor*), pode assumir qualquer valor dentro do intervalo $[0, 1]$. Quanto mais próximo γ estiver de 1, 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.

Este método também usa a equação 3.2 para agregar as informações de segunda mão e a equação 3.3 no cálculo final de reputação.

3.4.4 Média Exponencial Adaptada (*adapted_exponentialAverage*)

Como foi citado na seção 3.4.3, o mecanismo que usa média exponencial calcula o valor final da reputação através da equação 3.3. Sendo assim, as informações de segunda mão passam a ser desprezadas quando os históricos são preenchidos.

Nesta seção, apresenta-se o método de média exponencial adaptada, que sempre considerará as informações de segunda mão para o cálculo do valor final de reputação. Este método usa a equação 3.5 para agregar as informações de primeira mão, a equação 3.2 para agregar as informações de segunda mão e a equação 3.4 no cálculo final da reputação.

3.4.5 Método Exponencial sem Histórico (*enhancedReputation)*

O trabalho [7] apresenta um mecanismo de cálculo de reputação que não usa histórico de avaliações. A cada interação entre dois *peers*, a seguinte função é usada:

$$R(P_i, P_j) = (1 - \gamma) * R(P_i, P_j)_{current} + \gamma * e_{ij} \tag{3.6}$$

onde γ, é o fator de decaimento ou *fading factor* (vide Seção 3.4.3). $R(P_i, P_j)_{current}$ 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, o artigo propôs a seguinte função:

$$T(P_i, P_j) = \frac{\sum_{k=1}^{L} w_k * R(W_k, P_j)}{\sum_{k=1}^{L} w_k} \tag{3.7}$$

onde L é o número de testemunhas e w_k é a credibilidade (vide Seção 3.4.1) dada à informação de segunda mão recebida da testemunha W_k. w_k pode assumir qualquer valor dentro do intervalo $[-1, 1]$.

A utilização da equação 3.7 será desconsiderada por este trabalho, pois foram detectados alguns problemas em sua formulação. Primeiramente, o somatório colocado no denominador pode ocasionar uma divisão por zero. Ainda que fosse considerado que o autor quisesse, na verdade, fazer o somatório do número de testemunhas no lugar de suas credibilidades, outro problema aconteceria. A utilização de um intervalo $[-1, 1]$ de credibilidade levaria os clientes a considerarem de maneira não coerente as informações de segunda mão recebidas.

Como exemplo, considere que um cliente receba de uma testemunha uma informação de segunda mão de valor 0.6 e que esteja associando a esta testemunha um valor de credibilidade -0.7. O cliente, neste caso, que não confia na testemunha, considera o valor $-0.7 * 0.6 = -0.42$ no somatório executado no numerador da equação 3.7. Considere que a testemunha estivesse realmente mentindo e informando 0.6 como reputação de um provedor para o qual, na verdade, calculou 0.9. O cliente considerou um valor negativo, ainda menor que o informado pelo *peer* mentiroso. Se o cliente tivesse associado peso 1 à informação da testemunha mentirosa, não teria sido tão prejudicado!

Sendo assim, nas simulações executadas, assumiremos que o valor de credibilidade a ser usado pela equação de agregação das informações de segunda mão deve estar contido dentro do intervalo $[0, 1]$. Além disso, o denominador da equação será o número de testemunhas, evitando uma possível divisão por zero:

$$T(P_i, P_j) = \frac{\sum_{k=1}^{L} w_k * R(W_k, P_j)}{L} \tag{3.8}$$

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

Por fim, a equação 3.4 é usada para o cálculo do valor final de reputação.

3.4.6 Método da Teoria de Dempster-Shafer (*dst*)

A teoria de Dempster-Shafer (DST: *Dempster-Shafer Theory*) é descrita em [51] 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.

O importante é notar que com a introdução da incerteza, não ter crença na hipótese do bom comportamento de um dado *peer* não significa acreditar no seu mau comportamento, como acontece na teoria tradicional da probabilidade. Na teoria tradicional, se um *peer* P_i acredita que um *peer* P_j tem 0.6 de chance de ser mal comportado, isso significa que P_i acredita que P_j tem 0.4 de chance de ser bem comportado. Na DST, P_i poderia, por exemplo, ter 0.1 de crença no bom comportamento de P_j e 0.3 de incerteza.

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 $m(T)$, $m(notT)$ e $m(T, notT)$ 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:

$$m_{rs}(T) = \frac{m_r(T) * m_s(T) + m_r(T) * m_s(T, notT) + m_r(T, notT) * m_s(T)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \tag{3.9}$$

$$m_{rs}(notT) = \frac{m_r(notT) * m_s(notT) + m_r(notT) * m_s(T, notT) + m_r(T, notT) * m_s(notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \tag{3.10}$$

$$m_{rs}(T, notT) = \frac{m_r(T, notT) * m_s(T, notT)}{1 - (m_r(T) * m_s(notT) + m_r(notT) * m_s(T))} \tag{3.11}$$

Neste trabalho, estudaremos métodos de cálculo de reputação que usam a teoria de Dempster-Shafer tomando como base as propostas dos artigos [52], [11] e [12]. 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 seguinte função:

$$f(x_k) = g/\ H \tag{3.12}$$

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.

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

$$m(T) = \sum_{x_k=\Omega}^{1} f(x_k) \quad m(notT) = \sum_{0}^{x_k=\omega} f(x_k) \quad m(T, notT) = \sum_{x_k=\omega}^{x_k=\Omega} f(x_k) \tag{3.13}$$

As informações de segunda mão, que neste caso, são as crenças relacionadas ao comportamento de P_j que foram calculadas e informadas a P_i por outros *peers*, são agregadas através da regra de combinação de Dempster-Shafer (equações 3.9, 3.10 e 3.11).

Nas propostas dos trabalhos [52], [11] e [12], as informações de primeira mão **não** são agregadas às informações 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.

3.4.7 Método Adaptado da Teoria de Dempster-Shafer (*adapted_dst*)

Este mecanismo é uma adaptação do mecanismo dst. O cálculo das crenças a partir das informações de primeira mão é executado pelas equações 3.12 e 3.13 e o cálculo das crenças agregadas de segunda mão é executado através da regra de combinação de Dempster-Shafer (equações 3.9, 3.10 e 3.11).

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.

3.4.8 Método de Bayes (*bayes*)

O cálculo da reputação por método Bayesiano é utilizado por trabalhos como [43] e [44] no ambiente de redes *ad hoc*. A utilização deste método em ambientes P2P foi explorada por propostas como [8], [10] e [53]. Já o artigo [54], foca o seu estudo em ambientes de comércio eletrônico (*e-market*). Nesta dissertação, o método de Bayes será estudado através de um mecanismo baseado na proposta apresentada em [8].

Dado um *peer* P_i observando o comportamento de um outro *peer* P_j, existirá um parâmetro θ_{ij} que representará a probabilidade com a qual P_i "acha" que P_j irá se com-

portar bem. Enquanto P_i não interage com P_j, o valor de θ_{ij} é desconhecido. O trabalho [8] propõe que, neste caso, θ_{ij} assuma a forma de uma distribuição *a priori* ($Beta(\alpha, \beta)$) que é atualizada a cada nova interação de P_i com P_j.

Sendo assim, enquanto P_i e P_j não interagiram, $\theta_{ij} = Beta(1, 1)$. Depois, a cada nova interação que acontece entre estes dois *peers*, os valores de α e β são atualizados através das seguintes equações:

$$\alpha_{ij} = \alpha_{ij} + s \tag{3.14}$$

$$\beta_{ij} = \beta_{ij} + f \tag{3.15}$$

onde $s = 1$ se a interação é de sucesso e $s = 0$ se a interação é falha; $f = 1 - s$. A informação de primeira mão que P_i guarda de P_j são os valores de α_{ij} e β_{ij}.

O artigo [8] define ainda do uso de um fator de decaimento que resulta no seguinte cálculo de atualização da distribuição *a priori*:

$$\alpha_{ij} = u * \alpha_{ij} + s \tag{3.16}$$

$$\beta_{ij} = u * \beta_{ij} + f \tag{3.17}$$

onde a variável u é o fator de decaimento, que pode assumir valores dentro do intervalo $[0, 1]$. A utilização deste cálculo modificado de informações de primeira mão será estudado durante as simulações deste trabalho.

No que se refere à agregação das informações de segunda mão, as seguintes equações são usadas:

$$\alpha_w = \sum_{k=1}^{L} w_k * \alpha_{kj} \tag{3.18}$$

$$\beta_w = \sum_{k=1}^{L} w_k * \beta_{kj} \tag{3.19}$$

onde L é o número de testemunhas, α_w e β_w são os valores resultantes da agregação dos parâmetros α e β, respectivamente, fornecidos por cada testemunha. α_{kj} e β_{kj} constituem as informações dadas pela testemunha W_k a respeito de P_j. w_k é a credibilidade que é dada à informação de segunda mão recebida da testemunha W_k. w_k pode assumir qualquer valor dentro do intervalo $[0, 1]$.

É importante mencionar que, neste ponto, foi feita uma importante alteração na proposta original. O trabalho [8] propõe que seja feito um "teste de desvio" em cada informação de segunda mão recebida, estudado em detalhes na seção 3.7.2:

$$\|\mathbb{E}(Beta(\alpha_{kj}, \beta_{kj})) - \mathbb{E}(Beta(\alpha_{ij}, \beta_{ij}))\| \geq d \tag{3.20}$$

onde d é uma constante positiva chamada de limiar de desvio (*deviation threshold*).

Utilizando a proposta original, seriam utilizadas as seguintes equações:

$$\alpha_w = \sum_{k=1}^{L} w * \alpha_{kj} \tag{3.21}$$

$$\beta_w = \sum_{k=1}^{L} w * \beta_{kj} \tag{3.22}$$

onde w seria zero se o resultado do teste de desvio fosse positivo (informação de segunda mão descartada) e, w seria uma constante positiva se o resultado do teste fosse negativo.

A alteração do cálculo da agregação das informações de segunda mão foi necessária para tornar justa a comparação deste método com os demais estudados neste trabalho. Antes desta adaptação, este método [8] era o único a adotar uma utilização binária das informações de segunda mão: descartar as informações de segunda mão ou as considerar com um peso pré-definido. A modificação foi feita para que o método passasse a agregar as informações de segunda mão da mesma maneira que os demais métodos, ou seja, considerando os valores de credibilidades das testemunha como pesos dado às informações de segunda mão recebidas das mesmas.

Como será detalhado na seção 3.7.2, o mecanismo de credibilidade apresentado em [8] permite o cálculo de um valor de credibilidade dinâmico, que foi utilizado pelas equações 3.18 e 3.19 no lugar da proposta binária.

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

$$\alpha_f = \alpha_{ij} + \alpha_w \tag{3.23}$$

$$\beta_f = \beta_{ij} + \beta_w \tag{3.24}$$

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

$$\theta_{ij} = \mathbb{E}(Beta(\alpha_f, \beta_f)) \tag{3.25}$$

3.5 O Uso da Reputação Calculada

Nos mecanismos que usam média simples, explicados nas seções 3.4.1 e 3.4.2, e nos de média exponencial, explicados nas seções 3.4.3 e 3.4.4, o cálculo da reputação tem como resultado um valor dentro do intervalo $[0, 1]$. Já no mecanismo de método exponencial explicado na seção 3.4.5, o resultado é um valor dentro do intervalo $[-1, 1]$.

Apesar desta diferença, o uso do valor calculado de reputação no momento de julgar um *peer* é feito da mesma maneira em todos estes mecanismos. O valor de reputação calculado para um dado *peer* é simplesmente comparado com dois valores limiares pré-definidos, ω e Ω, no momento de concluir se este *peer* é ou não bem comportado.

Os valores adotados nas simulações dos mecanismos de intervalo $[0, 1]$ foram $\omega = 0.4$ e $\Omega = 0.6$. Nos mecanismos cujo intervalo de reputação é $[-1, 1]$, estes limites são convertidos para valores equivalentes através da fórmula abaixo:

$$valor = (valor * 2) - 1 \tag{3.26}$$

Se o valor de reputação calculado para um dado *peer* está abaixo de ω, ele é considerado mal comportado. Analogamente, se seu valor de reputação está acima de Ω, ele é considerado bem comportado.

O valor de reputação calculado poderá estar também dentro do intervalo $[\omega, \Omega]$, que não permitirá ao cliente que o calculou concluir nada a respeito do comportamento do provedor. Nestes casos, se o cliente tiver que decidir se irá ou não interagir com este provedor, sua postura será sempre a de arriscar. Caso contrário, numa rede P2P real, um *peer*, ao entrar numa rede, sendo desconhecido por todos e, portanto, com uma reputação inicial dentro do intervalo $[\omega, \Omega]$, nunca teria chance de interagir.

No caso dos métodos apresentados nas seções 3.4.6 e 3.4.7, é preciso definir como usar os três valores de crenças calculados para definir o comportamento de um *peer*. A solução apresentada pelos artigos [52] e [12] é comparar a diferença entre a crença no bom comportamento e a incerteza com um limiar pré-definido, ou seja:

$$m(T) - m(T, notT) \geq \rho \tag{3.27}$$

O resultado da diferença deve ser maior que o limiar ρ para que o *peer* seja julgado como bem comportado.

Essa abordagem apresenta problemas. Suponha, por exemplo, que um dado *peer* P_i calculou para outro *peer* P_j as crenças $m(T) = 0.6$, $m(notT) = 0.4$ e $m(T, notT) = 0$.

Neste caso, a diferença entre $m(T)$ e $m(T, notT)$ resultaria no valor 0.6. Suponha ainda que, P_i tenha calculado para outro *peer* P_k os valores de crenças $m(T) = 0.8$, $m(notT) = 0$ e $m(T, notT) = 0.2$. Neste último caso, a diferença entre $m(T)$ e $m(T, notT)$ também resulta no valor 0.6. A partir deste exemplo, é possível perceber que um *peer* cujo comportamento é tido como bom com 80% de certeza receberá o mesmo tratamento que outro cujo comportamento é tido como bom com 60% de certeza.

Por causa de problemas como este apresentados por esta abordagem, foi decidido usar uma outra solução. O artigo [11] apresenta uma maneira de converter os três valores de crenças em um valor único que expressa a probabilidade do *peer* se comportar bem. Uma vez que essa conversão tenha sido feita, o julgamento de um *peer* também poderá ser feito por simples comparação do valor de probabilidade calculado com valores limiares pré-definidos. A fórmula para conversão dos valores de crença num valor único de probabilidade é a seguinte:

$$prob(T) = \frac{m(T) + m(T, notT)}{1 + m(T, notT)} \tag{3.28}$$

Usando essa nova abordagem no exemplo dado anteriormente, o *peer* P_i teria calculado para P_j, cujas crenças eram $m(T) = 0.6$, $m(notT) = 0.4$ e $m(T, notT) = 0$, uma probabilidade $prob(T) = 0.6$. No caso do *peer* P_k, cujas crenças eram $m(T) = 0.8$, $m(notT) = 0$ e $m(T, notT) = 0.2$, a probabilidade calculada por P_i teria sido $prob(T) = 0.83$. Esse exemplo já mostra uma maior coerência, já que uma maior probabilidade de ser bem comportado foi associada ao *peer* com o maior valor de crença $m(T)$ e menor valor de crença $m(notT)$.

Com relação ao método Bayesiano descrito na seção 3.4.8, não há a mesma complicação apresentada no caso dos métodos que usam DST. A probabilidade θ de um dado *peer* se comportar bem é comparada com os limiares pré-definidos, exatamente como é feito para os demais mecanismos, e assim é possível julgá-lo como bem ou mal comportado.

3.6 Ataques aos Mecanismos de Reputação

Esta seção apresenta dois importantes ataques aos mecanismos de incentivo à cooperação baseados em reputação: O ataque do testemunho mentiroso e o ataque da mudança repentina de comportamento.

3.6.1 Ataque do Testemunho Mentiroso

Quando um *peer* P_i requisita informações a um *peer* P_k a respeito de um *peer* P_j, P_k deve repassar a P_i suas informações de primeira mão a respeito de P_j. Diz-se que o ataque do testemunho mentiroso acontece quando P_k repassa informações não compatíveis com as que possui de P_j.

O fato de um *peer* P_k, mentir para outros *peers* da rede no momento de testemunhar a respeito de *peers* com os quais interagiu não tem nenhuma relação com a maneira como ele se comporta como provedor de recursos/serviços. Este parece ser um conceito trivial, mas é muito importante para entender a necessidade do mecanismo de credibilidade.

Se o *peer* P_i partir da premissa que somente *peers* que são mal comportados mentem e então usar a reputação que calculou para P_k para dar peso às informações de segunda mão recebidas deste *peer*, estará cometendo um erro grave. Num ambiente em que os *peers* assumam esta premissa, testemunhas mentirosas poderão mentir ilimitadamente e possuir total credibilidade dos outros *peers* bastando, para isso, serem bons *peers* provedores. Para ter uma medida da honestidade de P_k, P_i precisa usar um mecanismo a parte, o mecanismo de credibilidade, visto na seção 3.7.

Com relação às manipulações que as testemunhas mentirosas fazem em suas informações de primeira mão no momento de mentir, o artigo [11] apresenta três modelos matemáticos de mentira:

Exagero Positivo - P_k manipula suas informações de primeira mão a respeito de P_j tentando fazê-lo parecer melhor provedor:

$$y = \sigma + x - \sigma * x \tag{3.29}$$

Exagero Negativo - P_k manipula suas informações de primeira mão a respeito de P_j, tentando fazê-lo parecer pior provedor:

$$y = x - \sigma * x/(1 - \sigma) \tag{3.30}$$

Mentira Complementar - P_k manipula suas informações de primeira mão a respeito de P_j, tentando fazer parecer que seu comportamento é o contrário do que ele calculou:

$$y = 1 - x \tag{3.31}$$

onde x é a informação de primeira mão que P_k possui de P_j; y é a informação de primeira mão manipulada por P_k e σ é uma constante no intervalo $[0, 1]$.

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 um ataque em conjunto à rede P2P. Trabalhos como [7], [13], [55], [56] e [57] citam o prejuízo que representa o ataque em conluio para o funcionamento das redes P2P.

Peers em conluio sempre difamarão *peers* que não estejam participando do conluio e elogiarão *peers* participantes do conluio. Supondo um conjunto de *peers* em conluio $\{P_{c1}, P_{c2}, ..., P_{cn}\}$ e *peers* P_i e P_j fora do grupo de conluio:

- Quando P_{c1} é consultado por P_i a respeito de P_j, difamará P_j (exagero negativo).
- Quando P_{c1} é consultado por P_i a respeito de P_{c2}, elogiará P_{c2} (exagero positivo).
- Quando P_{c1} é consultado por P_{c3}, a respeito de um *peer* fora ou dentro do conluio, apresentará a sua verdadeira informação de primeira mão, visto os *peers* estão em acordo e não mentem entre si.

Peers mal comportados podem tirar proveito de um ataque em grupo pois passam a contar com a divulgação de uma boa reputação associada a ele, feita por todos os outros participantes do grupo.

Vale acrescentar que, nesta dissertação, considera-se que *peers* participantes de conluio que necessitem de informações de segunda mão, somente as requisitarão de outros *peers* participantes do mesmo conluio, evitando, desta forma, a exposição à informações distorcidas, frutos do próprio ataque que estão promovendo

3.6.2 Ataque da Mudança Repentina de Comportamento

O ataque da mudança repentina de comportamento acontece quando um *peer* se comporta bem, de maneira a construir na rede uma reputação alta, e muda seu comportamento bruscamente. Este ataque tenta se aproveitar do tempo de convergência do mecanismo de incentivo baseado em reputação, ou seja, do tempo necessário para que a maior parte da rede perceba o comportamento do *peer*.

Depois que um *peer* muda repentinamente seu comportamento de bom para mau, os *peers* que foram seus clientes precisarão de algumas interações com ele para perceberem esta mudança, ou seja, para atualizarem e reduzirem seu valor de reputação de forma a refletir sua nova maneira de agir. Até que isso aconteça, os *peers* clientes deste provedor mal

comportado continuarão interagindo com ele, sendo vítimas de seu mau comportamento e divulgando a alta reputação que haviam calculado no período em que seu comportamento ainda era adequado.

3.7 Mecanismos de Credibilidade

Conforme foi visto na seção 3.6.1, os mecanismos de credibilidade têm o objetivo de tornar os *peers* da rede capazes de identificar que *peers* são honestos nos momentos de requisitar informações de segunda mão. Como já foi citado anteriormente, um dado *peer* P_i usará a credibilidade calculada para outro *peer* P_k como peso para toda informação de segunda mão recebida deste *peer*. Inicialmente, enquanto P_i não teve nenhuma oportunidade de avaliar a honestidade de P_k, acreditará nas informações de segunda mão deste *peer*, associando a ela peso 1.

Quando P_i requisitar informação a P_k a respeito de um outro *peer* P_j e decidir então interagir com este *peer*, poderá comparar o resultado desta interação com as informações recebidas. Esta comparação resultará num valor que irá quantificar o quão próximo da experiência com P_j foi a informação de segunda mão. Isso permitirá à P_i atualizar o valor da credibilidade associado a P_k.

Cada vez que P_i receber informação de segunda mão de P_k, ele dará a esta informação um peso igual à credibilidade atualizada de P_k e, depois da interação, repetirá o processo de comparação da experiência que teve com a informação que recebeu mantendo sempre atualizado o valor de credibilidade.

Alguns poucos trabalhos possuem um funcionamento um pouco diferente do descrito acima. Como exemplo, o trabalho [58], focado para aplicação em redes *ad hoc*, propõe um algoritmo conhecido como “maioria de votos”, no qual um *peer* compara as informações de segunda mão que recebeu entre si. Se P_i perceber, por exemplo, que a maioria das informações que recebeu aponta para o bom comportamento de P_j e uma única testemunha P_k acusou mau comportamento deste provedor, então P_i conclui que P_k é uma testemunha mentirosa.

Os diferentes algoritmos que podem ser usados nos mecanismos de credibilidade não serão foco de estudo deste trabalho. Aqui será considerado o algoritmo mais comumente usado e serão estudados dois diferentes métodos matemáticos de cálculo da credibilidade,

que estão detalhados nas seções a seguir (3.7.1 e 3.7.2).

3.7.1 *WMA - Weighted Majority Algorithm*

O trabalho [13], que apresenta dois mecanismos de cooperação (vide seções 3.4.1 e 3.4.3), propõe o uso do método de credibilidade que será descrito nesta seção. O trabalho [11] apresenta este mesmo método de credibilidade sendo usado em conjunto com o mecanismo de reputação que usa a teoria de Dempster-Shafer (vide 3.4.6).

Usando este método, quando um *peer* P_i requisitar informações de segunda mão a respeito de um *peer* P_j a outro *peer* P_k e decidir interagir com P_j, atualizará a credibilidade de P_k através das seguintes equações:

$$\theta = 1 - (1 - \beta) * \|R(P_k, P_j) - s\| \tag{3.32}$$

onde β é uma constante cujo valor está dentro do intervalo $[0, 1]$, $R(P_k, P_j)$ é a informação recebida de P_k a respeito de P_j e s é a avaliação que P_i deu a P_j na interação.

$$w_k = \theta * w_k \tag{3.33}$$

onde w_k é a credibilidade calculada para P_k

O valor de θ é determinado pela constante β e pela diferença entre a informação recebida de P_k e a avaliação dada por P_i à interação que acaba de fazer com P_j. Quanto maior for a diferença entre $R(P_k, P_j)$ e s, menor o valor de θ e, em conseqüência, menor a credibilidade de P_k.

No caso do mecanismo que usa método dst, quando P_k enviar a informação que possui a respeito de P_j, esta informação virá na forma das três crenças $m(T)$, $m(notT)$ e $m(T, notT)$. Neste caso, $R(P_k, P_j)$ será o resultado da equação 3.28 que converte as três crenças num valor único que expressa a probabilidade do *peer* de se comportar bem.

3.7.2 Método Bayesiano de Credibilidade

No artigo [8], foi apresentado um mecanismo de incentivo à cooperação baseado em reputação (vide seção 3.4.8) e um mecanismo Bayesiano de credibilidade. Suponha um *peer* P_i que requisita informação de segunda mão a respeito de um *peer* P_j a outro *peer* P_k e decide interagir com P_j. Na seção 3.4.8 foi descrito o "teste de desvio", feito através

da equação repetida a seguir:

$$\|\mathbb{E}(Beta(\alpha_{kj}, \beta_{kj})) - \mathbb{E}(Beta(\alpha_{ij}, \beta_{ij}))\| \geq d \tag{3.34}$$

onde d é uma constante positiva chamada de limiar de desvio (*deviation threshold*).

Se a diferença entre a informação recebida de P_k e a calculada por P_i a partir de suas experiências próprias com P_j for maior que um limiar d, então está caracterizado o testemunho mentiroso de P_k. Caso contrário, considera-se o testemunho de P_k como verdadeiro.

Considera-se que ϕ_{ik} é a probabilidade com a qual P_i "acha" que P_k será honesto. Inicialmente, P_i considera que ϕ_{ik} assume a forma de uma distribuição *a priori* $Beta(1, 0)$. O valor da credibilidade será atualizado a cada nova oportunidade que P_i tenha de avaliar a honestidade de P_k através das seguintes equações:

$$\gamma_{ik} = \rho * \gamma_{ik} + s \tag{3.35}$$

$$\delta_{ik} = \rho * \delta_{ik} + (1 - s) \tag{3.36}$$

onde s assume o valor 1 se provedor não passar no teste de desvio e 0 em caso contrário. ρ é o fator de decaimento (intervalo $[0, 1]$).

O valor final de credibilidade é então calculado através da seguinte equação:

$$\phi_{ik} = \mathbb{E}(Beta(\gamma_{ik}, \delta_{ik})) \tag{3.37}$$

Capítulo 4

O Simulador

Conforme foi descrito no capítulo 1, existem diversas propostas de mecanismos de incentivo baseados em reputação disponíveis na literatura. As diferenças de critérios, métricas e cenários usados na comprovação de desempenho das propostas dificulta a comparação entre os vários métodos matemáticos de cálculo de reputação existentes.

O desenvolvimento de aplicações P2P que façam uso de mecanismos de incentivo à cooperação baseados em reputação depende do melhor entendimento destes métodos matemáticos. Para este fim, foi desenvolvido, em linguagem C, um simulador capaz de gerar uma série de cenários nos quais os diferentes métodos podem ser testados e avaliados segundo os mesmos critérios e métricas, possibilitando comparações justas entre seus desempenhos.

A primeira seção apresenta os modos de funcionamento deste simulador e descreve como a ferramenta cria diferentes cenários a partir da configuração de um conjunto de parâmetros. A segunda seção descreve o algoritmo de simulação, ou seja, como os cenários gerados são utilizados pelo simulador para possibilitar a comparação entre os desempenhos dos métodos testados. Por fim, a última seção apresenta as métricas adotadas para avaliar os métodos.

A ferramenta de simulação desenvolvida foi utilizada neste trabalho para testar e comparar os métodos matemáticos de cálculo de reputação apresentados na seção 3.4 do capítulo 3. A implementação destes métodos no simulador levou em conta que cada um deles possui parâmetros específicos, necessários ao seu funcionamento, como será discutido nas seções que seguem.

4.1 A Geração de Cenários

Os *peers* de uma rede P2P real exercem simultaneamente os papéis de cliente e servidor (seção 2.1). Entretanto, neste ambiente, fica difícil interpretar que influências tem a adoção de um determinado método, pois a visão que um dado *peer* possui de outros participantes da rede é afetada, não somente pelo método de cálculo de reputação escolhido, mas também é uma resposta à visão que os outros *peers* têm a seu respeito, que por sua vez, depende de seu próprio comportamento.

Um *peer* julgado como mal, correta ou erradamente, não será mais atendido pelo *peer* que o julgou. Isso fará com que ele, não só calcule uma reputação de baixo valor para este *peer* que o julgou, como passe a divulgá-la (informação de segunda mão), exercendo influência na decisão de outros *peers* e inserindo uma realimentação a ser considerada na análise dos desempenhos dos métodos.

Sendo assim, ainda que esta escolha possa fazer com que os cenários gerados pelo simulador percam um pouco da dinâmica dos ambientes P2P reais, a maneira encontrada para isolar a influência do mecanismo de reputação, de modo a ter uma idéia clara das vantagens e desvantagens de cada método matemático, foi separar as funções de cliente e provedor.

Na ferramenta de simulação desenvolvida, os provedores não requisitam, somente disponibilizam recursos e, portanto, não têm motivos para não atender às requisições recebidas dos clientes. Tendo em vista que os provedores agirão apenas de acordo com o comportamento que lhes foi atribuído, os julgamentos executados pelos clientes dependerão apenas do desempenho do mecanismo de reputação. Quanto melhor o desempenho do método de cálculo de reputação, mais próximo do comportamento real de cada provedor será o comportamento calculado por cada cliente.

O total de clientes e provedores que constituirão os cenários gerados pelo simulador é configurável. Todo cenário é formado por uma quantidade `NUM_PEERS` de nós, dos quais `NUM_PRV` são provedores e o restante clientes.

Os cenários gerados no simulador assumem que cada cliente é capaz de identificar cada outro cliente e cada provedor presente na rede. Além disso, considera que, em caso de interesse, cada *peer* da rede pode estabelecer com qualquer outro *peer* uma comunicação direta. Para fazer uma analogia destas suposições com ambientes reais, duas aplicações de compartilhamento de arquivos são consideradas como exemplos: a

rede Napster [26] e a rede Gnutella [27].

Como foi visto na seção 2.3, no Napster, existe a presença de servidores de índices. Cada servidor possibilita aos *peers* conectados a ele se identificarem entre si, bem como descobrirem os *peers* que oferecem os arquivos de interesse. A seção 2.3 também descreveu o Gnutella. Neste aplicativo, os *peers* interessados em algum arquivo, fazem um *broadcast* de uma mensagem de busca, cujo alcance é limitado pelo campo TTL da mensagem (*Time To Live*). Os provedores dentro daquele alcance, que são capazes de fornecer tal arquivo, enviam uma resposta ao *peer* que o requisitou.

Os *peers* dos cenários gerados pelo simulador são análogos aos *peers* de uma rede Napster conectados a um mesmo servidor de índices e aos *peers* de uma rede Gnutella dentro de uma determinada área de alcance, ou seja, são capazes de identificar os *peers* a sua volta, escolher o provedor que considera mais indicado e as testemunhas que considera mais honestas.

Quanto ao comportamento dos provedores que constituem o cenário, o simulador permite configurar a quantidade de provedores bem e mal comportados. Os cenários gerados pelo simulador consideram que, dos NUM_PRV provedores existentes na rede, NUM_PRV_MAL_COMP são mal comportados e o restante é bem comportado. A ferramenta de simulação considera comportamento como sendo a probabilidade de um dado provedor atender a uma requisição de um serviço/recurso feita por um cliente. Os provedores mal comportados terão probabilidade PRV_PROB_MAL_COMP de atender às requisições feitas pelos clientes, enquanto que os provedores bem comportados atenderão às requisições que receberem com probabilidade PRV_PROB_BEM_COMP.

Outro importante aspecto relacionado ao comportamento é a simulação do ataque da mudança repentina de comportamento (seção 3.6.2). Os cenários gerados são compostos por MUDA_PRV provedores que mudam repentinamente de comportamento durante a simulação. Quando esta quantidade for maior que 0, o simulador sorteará aleatoriamente dentre os provedores bem comportados aqueles que mudarão de comportamento. A mudança ocorre sempre no meio da simulação, quando a maior parte dos clientes, senão todos, já terão calculado uma reputação de alto valor para estes provedores.

Durante a simulação, além de interagir com provedores e avaliá-los, os clientes também se comunicam entre si. Cada vez que um dado cliente necessita de informações a respeito de um provedor, requisita a uma quantidade NUM_TSTM de outros clientes. Foi

implementado no simulador dois modos ESCOLHA_TSTM que podem ser usados pelos clientes para escolherem suas testemunhas: escolha aleatória (distribuição uniforme) ou orientada por valores de credibilidade.

A escolha orientada por credibilidade só funciona em cenários onde os clientes estejam fazendo uso de um mecanismo de credibilidade. Neste modo, cada cliente se tornará capaz de gerenciar sua lista de testemunhas ordenada pela credibilidade e, no momento de escolher a quais delas requisitará informações de segunda mão, escolherá as NUM_TSTM com os maiores valores de credibilidade. Os dois mecanismos de credibilidade detalhados na seção 3.7 foram implementados no simulador.

Se o mecanismo de credibilidade MEC_CRED escolhido for o WMA, descrito na seção 3.7.1, o valor de β, usado pela equação 3.32 deve ser configurado. Já se MEC_CRED for o método Bayesiano de cálculo da credibilidade, estudado na seção 3.7.2, deverão ser configurados a constante d, conhecida por limiar de desvio (equação 3.20), e o fator de decaimento, usado nas equações 3.35 e 3.36. Estes parâmetros encontram-se resumidos na tabela 4.3 da seção 4.4.

O simulador considera que, além dos provedores, os clientes também pode ter diferentes comportamentos. Os clientes poderão ser mentirosos ou honestos nos momentos em que testemunharem. Cada cenário possuirá NUM_MENTIROSOS clientes mentirosos, escolhidos aleatoriamente, dentre o total de clientes que o constitui. Durante a simulação, cada vez que um mentiroso for escolhido como testemunha, a resposta será dada com informações falsas a respeito do provedor.

A seção 3.6.1 descreve três modelos matemáticos que podem ser usados por uma testemunha mentirosa para manipular suas informações de primeira mão de maneira a torná-las falsas: O exagero positivo (equação 3.29), o exagero negativo (equação 3.30) e a mentira complementar (equação 3.31). O simulador permite escolher qual dos três modelos será usado pelas testemunhas mentirosas.

Quando um modelo TIPO_MENTIRA é escolhido, todas as testemunhas mentirosas usam sua equação correspondente para manipular as informações de primeira mão antes de repassá-las ao cliente que as requisitou. As equações usadas pelos modelos exagero positivo e exagero negativo dependem da configuração do valor da constante σ, conforme mostram as equações 3.29 e 3.30.

O ataque da mentira em conluio também foi assunto da seção 3.6.1. O simulador

permite a simulação deste ataque a partir da definição do número de provedores (PRV_CONLUIO) e do número de clientes (CLT_CONLUIO) participantes do conluio. Assim, é possível gerar cenários contendo grupo de conluio formado por clientes e provedores e cenários com grupo de conluio constituído apenas por clientes.

Por fim, é importante detalhar como um determinado cenário, gerado a partir da definição das configurações descritas nesta seção, pode ser reutilizado em diferentes simulações com diferentes mecanismos de reputação. Esta é uma questão extremamente importante, pois visa possibilitar a comparação justa entre os diferentes mecanismos de reputação estudados neste trabalho. Se N diferentes cenários são gerados, todos os mecanismos devem ser simulados nos mesmo N cenários para que seus desempenhos sejam comparados.

A geração de um determinado cenário no simulador desenvolvido neste trabalho tem como saída um conjunto de arquivos de texto, que descrevem, detalhadamente, o cenário gerado. Estes arquivos, lidos durante a simulação, garantem que todos os mecanismos sejam testados exatamente nas mesmas condições. Um dos arquivos de saída detalha os provedores que constituem a rede. Neste arquivo constam as seguintes informações de cada provedor:

- Número identificador;
- Comportamento;
- Se o provedor mudará repentinamente de comportamento no meio da simulação;
- Se o provedor é participante de grupo de conluio.

Outro arquivo de saída detalha os clientes do cenário através das seguintes informações:

- Número identificador;
- Que tipo de modelo matemático será usado pelo cliente para manipular suas informações de primeira mão de forma a oferecer um testemunho mentiroso, caso o cliente em questão seja uma testemunha mentirosa;
- Se o cliente é participante de grupo de conluio.

O tempo de duração de cada simulação é definido pelo número de interações entre clientes e provedores, NUM_INTERACOES. O simulador escolhe aleatoriamente (distribuição uniforme) um cliente para participar de cada interação e gera um arquivo de saída com todos os resultados dessas escolhas.

Se a escolha das testemunhas usadas por cada cliente em cada interação é configurada como aleatória, a geração de cenário também tem como saída um arquivo com as testemunhas que serão consultadas pelos clientes em cada interação.

Já a definição do provedor que irá participar de cada interação, pode ser feita de duas maneiras, dependendo do modo de funcionamento ESCOLHA_PRV configurado no simulador: Simulação com provedor definido ou simulação com lista de provedores gerenciável pelo cliente.

Se o modo de funcionamento escolhido for provedor definido, o simulador escolherá aleatoriamente (distribuição uniforme) um provedor para cada interação da simulação e escreverá esta informação em um arquivo. Durante a simulação, este arquivo será lido e o cliente de cada interação decidirá, baseado na reputação que calculou para o provedor escolhido, se irá interagir ou não.

Nas simulações com lista de provedores gerenciável pelo cliente, o provedor de cada interação não é definido pela geração de cenário. Cada cliente é capaz de gerenciar uma lista de provedores ordenada por reputação. Durante a simulação, o cliente poderá então escolher o melhor provedor da lista e requisitar a ele o serviço/recurso desejado. Depois de cada interação, o cliente recalcula a reputação do provedor com o qual interagiu e o recoloca na lista, na posição devida, mantendo a lista ordenada por reputação.

Para fazer uma analogia destes dois modos com ambientes P2P reais, o modo provedor definido poderia ser comparado a uma rede com escassez de recursos, onde os *peers* encontram poucos provedores capazes de atendê-los e precisam decidir se irão ou não interagir. Já o modo de lista de provedores gerenciável poderia ser comparado a uma rede P2P com abundância de recursos, onde os *peers* encontram diversos provedores capazes de atendê-los e podem escolher a quem irão enviar suas requisições.

A tabela 4.1, da seção 4.4, apresentada ao final deste capítulo, resume os parâmetros que foram detalhados nesta seção e mostra ainda alguns valores que foram definidos nas simulações executadas por este trabalho, cujos resultados serão analisados no capítulo 5.

4.2 Simulação dos Métodos

Nesta seção, será descrito como os diferentes cenários, gerados a partir das configurações explicadas na seção 4.1, são usados nas simulações dos diferentes métodos matemáticos de reputação, estudados na seção 3.4.

As simulações começam com a leitura dos arquivos resultantes da geração de cenário (vide 4.1). Isso permitirá ao simulador conhecer quantas interações irão compor a simulação, que cliente participará de cada interação, se os clientes escolherão o provedor com o qual irão interagir ou se os provedores já estão definidos, se as testemunhas de cada interação serão escolhidas pelos clientes ou se já estão definidas, etc.

Em cada interação, a primeira providência do cliente escolhido será requisitar informações de segunda mão. Caso o cenário tenha sido gerado com o modo ESCOLHA_PRV configurado para provedor definido, o cliente requisitará informações de segunda mão a respeito apenas do provedor escolhido para a interação. Entretanto, se durante a geração do cenário foi configurado que o cliente gerenciará sua própria lista de provedores, então, ele requisitará informações a respeito de todos os *peers* de sua lista.

Manter-se recebendo informações de segunda mão atualizadas é muito importante para um dado *peer* que escolhe o provedor com o qual irá interagir. Desta maneira, ele poderá sempre recalcular e atualizar os valores de reputação dos demais *peers* da rede, até mesmo daqueles com os quais nunca interagiu. Numa rede P2P real, outros método de aquisição de informações de segunda mão podem ser adotados, entretanto, como não é o foco deste trabalho estudar a questão da escolha de um mecanismo eficiente para a troca de mensagens de segunda mão entre os participantes da rede, a implementação será então mantida conforme foi descrita acima, pois, para efeito de simulação e comparação dos mecanismos de reputação, é importante apenas que algum mecanismo de troca de mensagens seja adotado e utilizado nas simulações de todos os métodos de cálculo de reputação.

No momento em que receber as informações de segunda mão, o cliente as agregará através de equações do método de reputação que estiver usando. Depois, agregará os resultados desta etapa com suas próprias informações (informações de primeira mão), chegando então ao valor final de reputação de cada um dos provedores de quem pediu informação (apenas um provedor no caso do modo de simulação com provedor definido).

Se o modo de simulação for com provedor definido, a reputação calculada será uti-

lizada pelo cliente para decidir se irá ou não requisitar o serviço/recurso ao provedor daquela interação. Já se o modo de simulação for com lista gerenciável de provedores, o cliente usará as reputações para escolher o provedor de maior reputação. Caso o provedor de maior reputação possua uma reputação que o classifique como bem comportado, o cliente o enviará sua requisição de serviço. Caso contrário, desistirá da interação visto que se o melhor provedor de sua lista é mal comportado não existe quem possa atendê-lo.

Uma vez que o cliente tenha interagido com um provedor, a próxima ação do cliente será avaliá-lo. Na seção 3.2 foi explicado que a representação numérica desta avaliação varia entre os mecanismos. Nos mecanismos explicados nas seções 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.6 e 3.4.7, as avaliações são dadas dentro do intervalo $[0, 1]$. No mecanismo detalhado na seção 3.4.5, o valor de avaliação é dado dentro do intervalo $[-1, 1]$. Já para o mecanismo da seção 3.4.8, a avaliação é binária, ou seja, 1 ou 0 (sucesso ou falha).

Para tornar possível a execução de testes e a comparação de todos os métodos de cálculo de reputação, mesmo diante destas diferenças, o simulador fará uso de alguns artifícios. Primeiramente, o resultado da interação, que pode ser sucesso ou falha, é gerado pelo simulador de acordo com o comportamento definido para o provedor. Por exemplo, se o provedor tem um comportamento 0.9, o simulador irá gerar um resultado para esta interação que tem 90% de chance de ser sucesso e 10% de chance de ser falha. A partir deste resultado, o cliente que participou da interação gerará um valor de avaliação seguindo os seguintes passos:

- Se o resultado for sucesso, escolhe uma avaliação dentro do intervalo $[0.6, 1]$.
- Se o resultado for falha, escolhe uma avaliação dentro do intervalo $[0, 0.4]$.
- Verifica se o mecanismo de reputação que está sendo usado utiliza o intervalo de valores para avaliação $[0, 1]$. Caso não utilize, a avaliação dada deverá sofrer uma conversão para o intervalo correto de valores. Se o intervalo em uso for $[-1, 1]$ o valor pode ser convertido através da equação 3.26. Já se o método for Bayesiano, a avaliação dada será 1 em caso de sucesso e 0 em caso de falha.

Numa rede P2P real, esta avaliação seria feita pelo cliente com base em um critério de avaliação definido (vide seção 3.2). Porém, o foco deste trabalho é o estudo dos mecanismos descentralizados de incentivo à cooperação baseados em reputação aplicados em redes P2P, não numa aplicação específica destas redes. Já que o simulador

não tenta reproduzir nenhuma aplicação específica não existe maneira de definir um critério para avaliação, mas é importante que o simulador reproduza as variações de satisfação/insatisfação que os clientes têm em suas avaliações.

Foi dito que, dado o comportamento do provedor, ou seja, a probabilidade de atender ou não a requisição do cliente, o simulador gera um resultado para iteração, que será sucesso ou falha. Quando este resultado é definido, também é definido o intervalo no qual deverá se dar a avaliação feita pelo cliente, $[0.6, 1]$ ou $[0, 0.4]$. A avaliação gerada para o provedor é então um valor escolhido aleatoriamente dentro de um destes intervalos. Por facilidade de implementação, foram serão considerados valores discretos. Se o resultado for sucesso, a avaliação será escolhida aleatoriamente (distribuição uniforme) dentre os possíveis valores $0.6, 0.7, 0.8, 0.9, 1.0$. Se o resultado for falha, a avaliação será escolhida aleatoriamente dentre os possíveis valores $0, 0.1, 0.2, 0.3, 0.4$.

Quanto ao valor 0.5, entende-se que seria uma avaliação neutra, usada nos casos em que o cliente não pode, por algum motivo, avaliar o provedor com o qual interagiu. Se existirá ou não uma condição capaz de gerar dúvida num cliente a respeito do comportamento de um provedor, dependerá de dois fatores: A aplicação em que a rede P2P estiver sendo usada e o critério de avaliação que estiver sendo adotado pelos *peers* da rede.

Numa aplicação P2P de compartilhamento de arquivos de áudio em que o critério de avaliação adotado seja a qualidade do áudio, será pequena a possibilidade de um usuário não conseguir avaliar a qualidade do áudio adquirido de um provedor. Entretanto, se o critério de avaliação fosse velocidade de *download* do provedor, um cliente que estivesse com problemas de intermitência em sua conexão, poderia se sentir impedido de avaliar se foi boa ou não a velocidade com a qual adquiriu o arquivo.

Nas seções 3.4.6 e 3.4.7, foram apresentados mecanismos que usam a DST no cálculo da reputação. Foi citado que uma das grandes diferenças deste para os métodos probabilísticos é a capacidade, dada pela aplicação da teoria de Dempster-Shafer, de manipular de maneira explícita a incerteza. Para estudar se existe alguma vantagem destes métodos em cenários como o citado acima, onde um cliente pode não conseguir avaliar um provedor, o simulador permite a configuração de uma probabilidade de falha na avaliação FALHA_AVALIACAO. Ao final de uma interação, seja ela de sucesso ou não, a avaliação feita pelo cliente falhará com probabilidade FALHA_AVALIACAO.

Depois que um cliente interage e avalia um provedor, seja esta avaliação boa, ruim ou

neutra, ele deverá atualizar a credibilidade de suas testemunhas e a reputação do provedor com o qual interagiu. Caso o modo de simulação seja com provedor definido, depois de executar estas atualizações, o cliente dará como encerrada a interação.

Já se o simulador estiver trabalhando no modo de lista gerenciável de provedores, o final da interação pode não acontecer no fim da primeira tentativa do cliente de conseguir o serviço que deseja. Neste caso, se o cliente não obtiver sucesso com o provedor escolhido, ele consultará novamente sua lista e analisará a reputação do próximo provedor melhor posicionado. Caso a reputação deste provedor o caracterize como mal comportado, o cliente perceberá que não há mais tentativas que possa fazer e dará por terminada a interação. Caso contrário, requisitará o serviço a este provedor.

Neste modo, a interação será finalizada pelo cliente quando ele obtiver sucesso, ou quando não houver mais provedores bem comportados em sua lista a quem ele possa enviar uma nova requisição do recurso que deseja.

O objetivo das simulações no modo de provedor definido é uma comparação bastante rígida entre os métodos. Já foi detalhado que, neste modo, o cliente e provedor de cada interações são lidos de arquivos gerados na fase de geração do cenário e, portanto, são os mesmos nas simulações de cada método. Além disso, antes de simular os métodos de reputação num dado cenário, o simulador gera um arquivo com um resultado (sucesso ou falha) para cada interação e uma correspondente avaliação a ser dada pelo cliente participante de 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 aqueles especificados neste arquivo.

A geração do arquivo de resultados e avaliações antes das simulações dos métodos num dado cenário garante que todas as interações que forem consumadas durante cada simulação de cada método serão idênticas - mesmo cliente, mesmo provedor, mesmo resultado, mesma avaliação. A diferença entre as simulações dos métodos estará justamente na decisão de consumar ou não a interação que será tomada pelo cliente. Tendo em vista que esta decisão é inteiramente baseada na reputação que este cliente calculou, ela dependerá totalmente do método matemático em uso. Métodos de cálculo de reputação eficientes proporcionarão aos clientes decisões mais acertadas.

As simulações em modo com lista de provedores gerenciáveis têm como objetivo comparar os métodos num ambiente mais flexível, onde o cliente, além do poder de de-

cisão (interagir ou não com um dado provedor), possui o poder de escolha do provedor com o qual irá interagir. Dependendo do método que estiver sendo simulado, a ordem das listas gerenciadas por cada cliente será diferente. Métodos de cálculo de reputação eficientes proporcionarão aos clientes uma ordenação justa de suas listas e evitarão repetidas tentativas para conseguir o recurso que deseja.

4.2.1 Implementação dos Mecanismos de Reputação

A simulação do método de média simples para o cálculo de reputação, detalhado na seção 3.4.1, exige a configuração do tamanho dos históricos H que cada cliente manterá para guardar as avaliações mais recentes de cada provedor. Para a simulação do método adaptado de média simples, descrito na seção 3.4.2, além de configurar o tamanho dos históricos, será necessário definir o valor do peso α que será dado à informação de primeira mão na equação 3.4.

O método de média exponencial também precisa da configuração de tamanho dos históricos H e, além disso, exige a definição do fator de decaimento γ, usado pela equação 3.5. Estas configurações também são necessárias para a simulação do método adaptado exponencial, que, precisa ainda, da definição do peso da informação de primeira mão α usado pela equação 3.4. O método exponencial sem histórico, detalhado na seção 3.4.5, exige a configuração do fator de decaimento γ e deste peso α dado às informações de primeira mão.

A simulação dos mecanismos detalhados nas seções 3.4.6 e 3.4.7 exigem apenas que seja configurado o tamanho H que terão os históricos de avaliações. Por fim, o método Bayesiano, estudado na seção 3.4.8, só precisa de configuração, caso haja interesse em ter o efeito de decaimento do peso das avaliações antigas na agregação das informações de primeira mão, conseguido pelo uso do fator de decaimento u das equações 3.16 e 3.17. Neste caso, o fator de decaimento deve ser diferente de 1.

A tabela 4.2, da seção 4.4, apresentada ao final deste capítulo, resume todos estes parâmetros.

4.3 Métricas para Avaliação dos Métodos

Esta seção apresenta as métricas implementadas no simulador para avaliar os métodos matemáticos de cálculo de reputação testados.

4.3.1 Percentual de Decisões Acertadas

Diz-se que um *peer* toma uma decisão acertada quando escolhe não interagir com um provedor mal comportado ou interagir com um bem comportado [7]. O percentual de decisões acertadas D de uma dada simulação é calculado por:

$$D = \frac{\sum_{i=1}^{C} d_i}{\sum_{i=1}^{C} n_i} \tag{4.1}$$

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

4.3.2 Reputação Média

O simulador calcula a reputação média dos provedores bem e mal comportados e dos provedores que aplicam o ataque da mudança repentina de comportamento [7], [12].

$$R = \frac{\sum_{i=1}^{P} \frac{\sum_{k=1}^{C} Rep(k,i)}{C}}{P} \tag{4.2}$$

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 for a dos provedores bem comportados, então P é o número de provedores bem comportados. Se R for reputação média dos provedores mal comportados, então P é o número de provedores mal comportados. Se R for a reputação média dos provedores que praticam o ataque da mudança repentina de comportamento, então P é o número de provedores que praticam o ataque da mudança repentina de comportamento.

4.3.3 Percentual Médio de Provedores Identificados

Diz-se que um cliente identificou um provedor bem comportado quando calculou sua reputação maior ou igual ao valor limite que define bom comportamento. Da mesma forma, diz-se que um cliente identificou um provedor mal comportado quando a reputação

calculada para este provedor foi menor ou igual ao valor limite que define mal comportamento [43]. O percentual médio de provedores bem comportados identificados é calculado pela seguinte equação:

$$Id = \frac{\sum_{i=1}^{C} p_i /\ P}{C} \tag{4.3}$$

onde C é a quantidade de clientes da rede, p_i é a quantidade de provedores bem comportados identificados pelo cliente i e P é a quantidade total de provedores bem comportados da rede. Para o cálculo do percentual médio de provedores mal comportados identificados, p_i representaria a quantidade de provedores mal comportados identificados pelo cliente i e P seria o total de provedores mal comportados.

4.3.4 Percentual de Tentativas de Sucesso

Esta é uma métrica exclusiva do modo de operação do simulador no qual cada cliente é capaz de gerenciar sua lista de provedores ordenada por reputação. Neste modo, os clientes poderão fazer mais de uma tentativa de conseguir o recurso/serviço desejado. O simulador permite calcular o percentual de tentativas de sucesso:

$$S = \frac{\sum_{i=1}^{C} s_i}{\sum_{i=1}^{C} t_i} \tag{4.4}$$

onde C é o número de clientes da rede, s_i é o número de tentativas de sucesso feitas pelo cliente i e t_i é o número total de tentativas do cliente i.

O simulador também calcula o percentual médio de tentativas de sucesso de cada cliente através da equação abaixo:

$$S_m = \frac{\frac{\sum_{i=1}^{C} s_i}{\sum_{i=1}^{C} t_i}}{C} \tag{4.5}$$

4.3.5 Percentual de Interações Perdidas

No modo de simulação com lista gerenciável de provedores, um cliente que esteja associando baixos valores de reputação a provedores bem comportados, os posicionarão no fim de sua lista e pode desistir do recurso/seviço desejado concluindo, equivocadamente, que não há mais provedores bem comportados em sua lista aos quais poderia requisitá-lo. O simulador permite calcular o percentual de interações desperdiçadas pelos clientes:

$$Ip = \frac{\sum_{i=1}^{C} p_i}{I} \tag{4.6}$$

onde C é o número de clientes da rede, p_i é o número de interações desperdiçadas pelo cliente i e I é o número total de interações da simulação.

O simulador também calcula o percentual médio de interações desperdiçadas por cada cliente ao longo da simulação:

$$Ip_m = \frac{\frac{\sum_{i=1}^{C} p_i}{I}}{C} \tag{4.7}$$

4.3.6 Credibilidade Média

O cálculo do valor médio de credibilidade dos clientes que testemunham corretamente é feito através da equação a seguir [11]:

$$Cred = \frac{\sum_{i=1}^{W} \frac{\sum_{k=1}^{C} Cred(k,i)}{C-1}}{W} \quad \forall\, k \neq i \tag{4.8}$$

onde W é o número de clientes que testemunham corretamente, C é o número de clientes da rede, $Cred(k, i)$ é a credibilidade que o cliente k calculou para o cliente i. Para o cálculo da credibilidade média dos clientes que aplicam o ataque do testemunho mentiroso, W é o número de clientes mentirosos.

4.4 Resumo de Parâmetros do Simulador

As tabelas a seguir resumem os principais parâmetros configuráveis do simulador e mostram alguns valores que foram considerados nas simulações, cujos resultados são apresentados e analisados ao longo do capítulo 5.

Uma observação importante é que foram feitas simulações com o parâmetro `NUM_PRV` configurado para maiores valores, ou seja, o percentual de *peers* provedores foi variado. Entretanto, somente os resultados com o valor 10 serão mostrados. O aumento do percentual de provedores presentes na rede causa apenas um aumento do tempo de convergência dos métodos, pois os clientes têm mais provedores com os quais podem interagir e demoram um número maior de interações para acumularem experiências com todos.

Tabela 4.1: Parâmetros Gerais de Simulação

Parâmetro	**Significado**	**Valor**
NUM_PEERS	total de *peers*	100
NUM_PRV	número de provedores	10
NUM_PRV_MAL_COMP	número de provedores mal comportados	5
PRV_PROB_BEM_COMP	comportamento dos provedores bem comportados	0.9
PRV_PROB_MAL_COMP	comportamento dos provedores mal comportados	0.1
MUDA_PRV	número de provedores que mudam de comportamento	1 nas simulações que testam este ataque
NUM_TSTM	número de testemunhas por interação	5
ESCOLHA_TSTM	modo de escolha das testemunhas	modo aleatório ou orientado por credibilidade
NUM_MENTIROSOS	número de testemunhas mentirosas	valor menor ou igual ao total de clientes
TIPO_MENTIRA	modelo de mentira utilizado	exagero positivo, exagero negativo ou mentira complementar
PRV_CONLUIO	número de provedores em conluio	5
CLT_CONLUIO	número de clientes em conluio	valor menor ou igual ao número de mentirosos
MEC_CRED	mecanismo de credibilidade	WMA ou método Bayesiano
NUM_INTERACOES	total de interações	120000
ESCOLHA_PRV	modo de escolha do provedor de cada interação	modo aleatório ou de lista de provedores gerenciável
FALHA_AVALIACAO	probabilidade do cliente não conseguir avaliar o provedor	$[0, 1]$
σ	constante usada pelos modelos de exagero	0.4 na maior parte das simulações

Tabela 4.2: Parâmetros dos Mecanismos de Reputação Testados

Parâmetro	**Significado**	**Métodos que Utilizam**	**Valor**
H	histórico de avaliações	simpleAverage, adapted_simpleAverage, exponentialAverage, adapted_exponentialAverage, dst, adapted_dst	simulações com valores 10 e 100
α	peso associado às informações de primeira mão	adapted_simpleAverage, adapted_exponentialAverage, enhancedReputation	simulações com valores 0.5, 0.6 e 0.7
γ	fator de decaimento	exponentialAverage, adapted_exponentialAverage, enhancedReputation	0.6 na maior parte das simulações
u	fator de decaimento do método Bayesiano	bayes	1 na maior parte das simulações

Tabela 4.3: Parâmetros dos Mecanismos Credibilidade

Parâmetro	**Significado**	**Métodos que Utilizam**	**Valor**
β	constante usada pela equação 3.32	WMA	simulações com valores 0.9 e 0.6
d	limiar de desvio	Método Bayesiano de Credibilidade	simulações com valores 0.1 e 0.3
ρ	fator de decaimento	Método Bayesiano de Credibilidade	simulações com valores 1, 0.9 e 0.6

Capítulo 5

Resultados dos Testes

Este capítulo traz a descrição dos resultados obtidos das simulações dos oito métodos apresentados no capítulo 3. Para facilitar a visualização dos resultados, ao invés de gráficos contendo oito curvas, serão usadas figuras com dois gráficos, cada um contendo curvas de quatro mecanismos.

A legenda utilizada nos gráficos associará a cada método os nomes que são mostrados entre parênteses nos títulos das seções que os detalham (capítulo 3). Esta nomeclatura é repetida na tabela 5.1 a seguir. A simulação de cada método em cada cenário foi repetida 10 vezes para geração dos intervalos de confiança.

Tabela 5.1: Nomeclatura Utilizada nos Gráficos

Método	**Nome**
Média Simples (Seção 3.4.1)	simpleAverage
Média Simples Adaptada (Seção 3.4.2)	adapted_simpleAverage
Média Exponencial (Seção 3.4.3)	exponentialAverage
Média Exponencial Adaptada (Seção 3.4.4)	adapted_exponentialAverage
Método Exponencial sem Utilização de Histórico (Seção 3.4.5)	enhancedReputation
Método da Teoria de Dempster-Shafer (Seção 3.4.6)	dst
Método Adaptado da Teoria de Dempster-Shafer (Seção 3.4.7)	adapted_dst
Método de Bayes (Seção 3.4.8)	bayes

Ainda a respeito dos gráficos, é importante mencionar que, como a representação numérica da reputação calculada pelo método exponencial sem histórico (seção 3.4.5)

pertence ao intervalo $[-1, 1]$, foi feito, somente para os gráficos de reputação média, uma normalização, para o intervalo $[0, 1]$, dos valores mostrados. Todos os cálculos executados por este método respeitaram seu intervalo de valores $[-1, 1]$ e, somente no momento de traçar suas curvas de reputação média, a normalização foi executada com o intuito de facilitar a análise e comparação com os demais métodos.

Deve ser lembrado ainda que, no caso do método dst, as crenças são convertidas em um valor de probabilidade (vide Seção 3.5) e, sendo assim, os gráficos mostram este valor como sendo a reputação calculada por este método.

Outro importante aspecto da seção 3.5 que deve ser mencionado é a forma como os clientes julgam os provedores com os quais interagem. Provedores com reputação abaixo do limite $\omega = 0.4$ são considerados mal comportados e provedores com reputação acima do limite $\Omega = 0.6$ são considerados bem comportados. No caso do método *enhanceReputation*, estes valores limites são convertidos através da fórmula 3.26 para os valores $\omega = -0.2$ e $\Omega = 0.2$, respectivamente.

Os desempenhos dos métodos foram testados em sete diferentes cenários gerados pelo simulador. Os resultados obtidos a partir do conjunto de simulações feitas em cada um destes cenários são apresentados nas sete seções a seguir.

O Cenário 1 apresenta simulações com baixa complexidade. O simulador é configurado no modo de provedor definido, a rede não possui *peers* executando o ataque da mudança repentina de comportamento, nenhum mecanismo de credibilidade é usado, as testemunhas são escolhidas aleatoriamente, não há *peers* aplicando o ataque do testemunho mentiroso e os clientes não falham nos momentos de executarem suas avaliações.

O Cenário 2 mantém todas as características do Cenário 1, exceto que os clientes podem falhar na avaliação dos provedores ao final das interações. O Cenário 3 testa o ataque da mudança repentina de comportamento e, portanto, mantém quase todas as características do Cenário 1, diferenciando-se apenas pela presença de um provedor que muda de comportamento durante a simulação.

Já o ataque do testemunho mentiroso é testado pelo Cenário 4, que conta com a presença de *peers* mentirosos e mantém todas as outras características do Cenário 1. O ataque da mentira em conluio é testado pelo Cenário 5, que também conta com a presença de mentirosos, mas considera que os mesmos constituem um grupo de conluio.

O uso dos mecanismos de credibilidade é testado no Cenário 6. Neste cenário, as

testemunhas não são escolhidas aleatoriamente, mas cada cliente é o responsável por escolher suas testemunhas a partir de sua lista de testemunhas ordenada por credibilidade. Dois mecanismos de credibilidades apresentados na seção 3.7 foram testados.

O Cenário 7 testa os métodos no modo de simulação com lista gerenciável de provedores. Esta seção conta, na verdade, com um conjunto de cenários neste modo de simulação. No primeiro conjunto de simulações foi considerado que não existiam testemunhas mentirosas na rede e as testemunhas de cada interação eram escolhidas aleatoriamente. As simulações seguintes admitiram a presença de clientes mentindo e, por fim, foram considerados ambientes cujos clientes eram capazes de escolher suas próprias testemunhas a partir do uso de um mecanismo de credibilidade.

A última seção deste capítulo apresenta, resumidamente, as principais observações feitas ao longo da análise dos resultados obtidos.

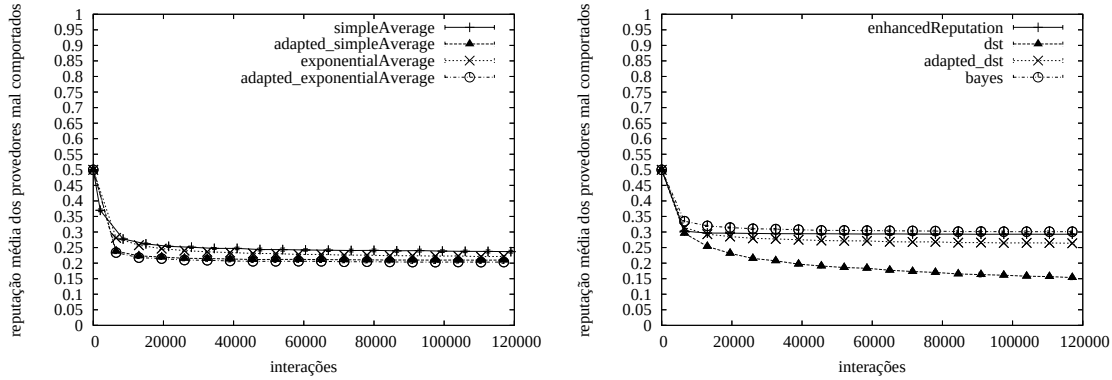
5.1 Cenário 1 - Provedores Mal Comportados

O primeiro cenário de simulação é bastante simples. O simulador está configurado para o modo de provedores definidos, metade dos provedores são mal comportados, não há provedores que aplicam o ataque da mudança repentina de comportamento, as testemunhas são escolhidas aleatoriamente durante a geração de cenário, não há clientes aplicando o ataque do testemunho mentiroso e os clientes não falham no momento de avaliar os provedores [59].

Este cenário foi simulado, primeiramente, considerando que, nas simulações de métodos que usam históricos de avaliações, cada *peer* guarda no máximo 10 avaliações mais recentes de cada provedor com o qual interagiu. Também foi configurado, para o caso dos métodos que usam a equação 3.4 no cálculo final da reputação, o peso associado às informações de primeira mão α igual a 0.5, ou seja, foi dado às informações de segunda mão peso igual ao das informações de primeira mão.

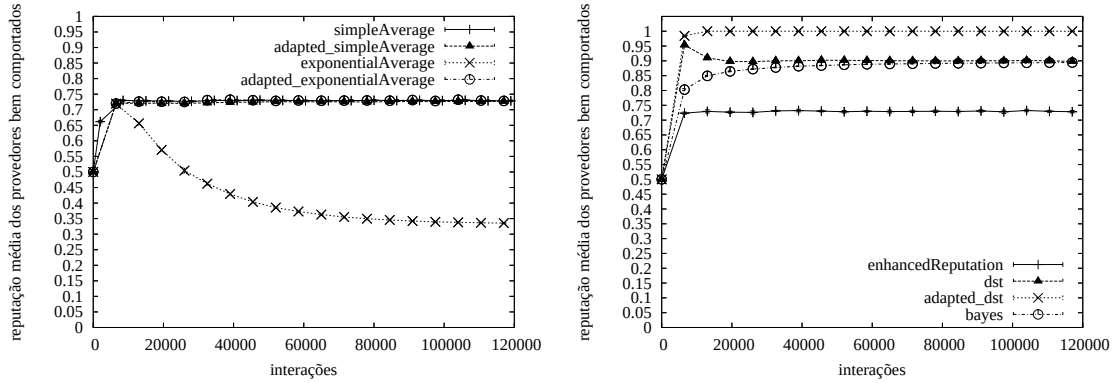
As figuras 5.1 e 5.2 apresentam as curvas de reputação média dos provedores mal e bem comportados. Já as figuras 5.3 e 5.4 mostram o percentual médio de provedores mal e bem comportados identificados. As simulações feitas para construção destes gráficos consideraram, no caso dos métodos que fazem uso de fator de decaimento, um valor igual a 0.6 para esta constante. Este é o valor comumente considerado pelos trabalhos que

propõem o uso deste parâmetro na agregação das informações de primeira mão.



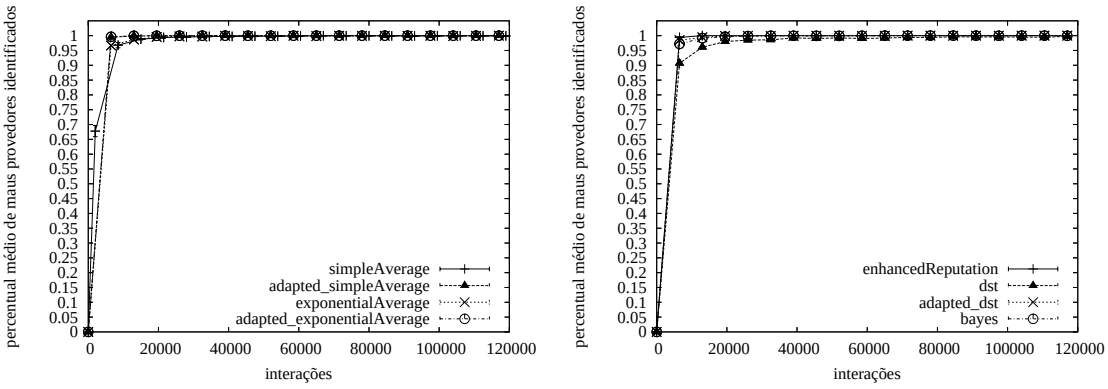
(a) (b)

Figura 5.1: H = 10 - Reputação Média dos Provedores Mal Comportados



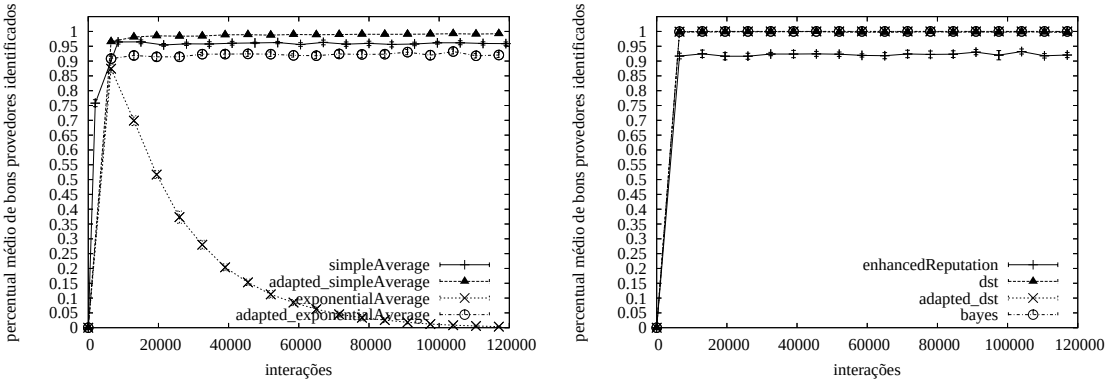
(a) (b)

Figura 5.2: H = 10 - Reputação Média dos Provedores Bem Comportados



(a) (b)

Figura 5.3: H = 10 - Percentual Médio de Maus Provedores Identificados



(a) (b)

Figura 5.4: H = 10 - Percentual Médio de Bons Provedores Identificados

As figuras 5.1 e 5.3 mostraram que nenhum método apresentou problemas na identificação de provedores mal comportados neste cenário. Já com relação à identificação dos provedores bem comportados, são necessárias algumas considerações.

De acordo com o que pode ser observado na figura 5.2, depois de um período transitório, os métodos estabilizaram em um valor médio de reputação para os provedores bem comportados dentro do intervalo de valores que é indicativo de bom comportamento. A única exceção foi o método exponencial, que apresentou uma queda brusca no valor médio de reputação e estabilizou em um valor indicativo de mau comportamento.

O uso de um histórico de apenas 10 avaliações em conjunto com a utilização do fator de decaimento aumenta muito o peso das avaliações mais recentes, conseqüentemente aumenta bastante a rapidez de convergência do método. Poucas falhas cometidas pelos *peers*

avaliados tornam-se suficientes para resultar em um baixo valor calculado na agregação das informações de primeira mão. Tendo em vista que mesmo provedores bem comportados têm algum percentual de chance de não conseguir atender às requisições de seus clientes, esta convergência demasiadamente rápida pode causar julgamentos injustos.

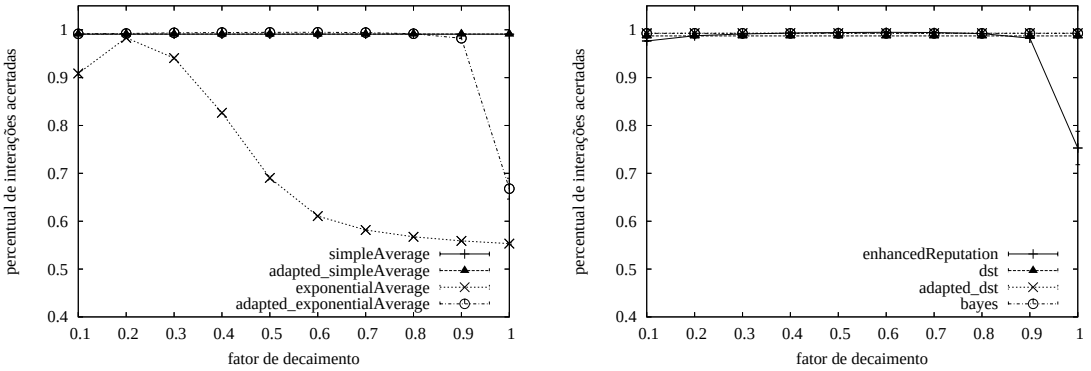
O método exponencial adaptado também usa histórico e fator de decaimento, mas suas curvas mostram um desempenho superior ao do método exponencial original. Isso acontece porque o método adaptado não utiliza a equação 3.3, que faz com que as informações de segunda mão sejam desconsideradas quando os históricos são preenchidos. O uso da equação 3.4 pelo método exponencial adaptado possibilita que a exagerada rapidez de convergência em sua agregação das informações de primeira mão seja amenizada pelas informações de segunda mão.

A figura 5.4 também aponta para o fato de que somente o método exponencial apresentou uma queda brusca no percentual médio dos provedores bem comportados identificados, demonstrando que estes provedores deixaram, ao longo da simulação, de serem considerados bem comportados.

Para estudar um pouco melhor o efeito da variação do fator de decaimento nos métodos que o utilizam, a simulação deste cenário foi repetida para diversos valores desta constante. A figura 5.5 mostra que, nesta configuração, o aumento no fator de decaimento faz reduzir o percentual de acertos do método exponencial. Já os métodos exponenciais que sempre fazem uso das informações de segunda mão (mesmo depois do preenchimento dos históricos de avaliações) só foram afetados quando fatores de decaimento com valores muito altos foram adotados.

A figura 5.5 mostra ainda que, somente quando o fator de decaimento adotado possui valores muito baixos, o método exponencial original consegue aproximar seu percentual de acertos dos demais métodos exponenciais, demonstrando mais uma vez que este método, por deixar de usar as informações de segunda mão, se torna bem mais sensível a convergência exagerada do cálculo de primeira mão.

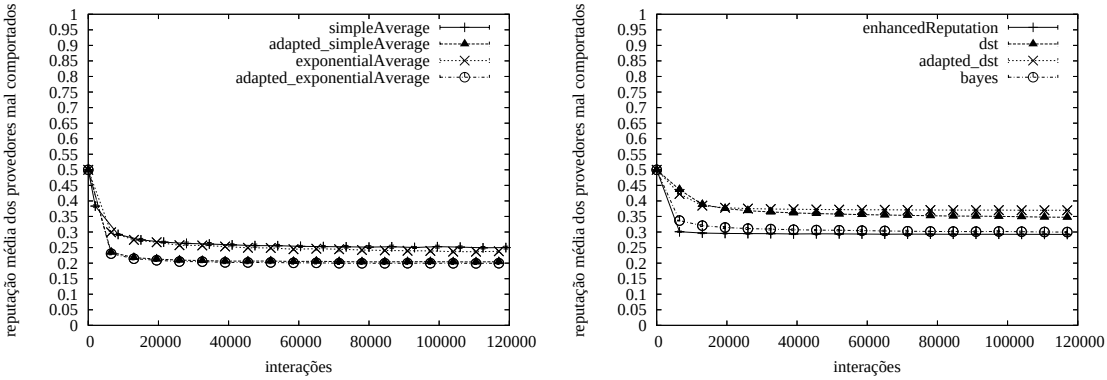
Quanto aos métodos que não usam o fator de decaimento, foram mantidos nestes gráficos para que seus respectivos percentuais de decisões acertadas (constantes por não serem afetados pelo parâmetro variado) pudessem ser comparados com os percentuais dos demais métodos afetados pela variação desta constante.



(a) (b)

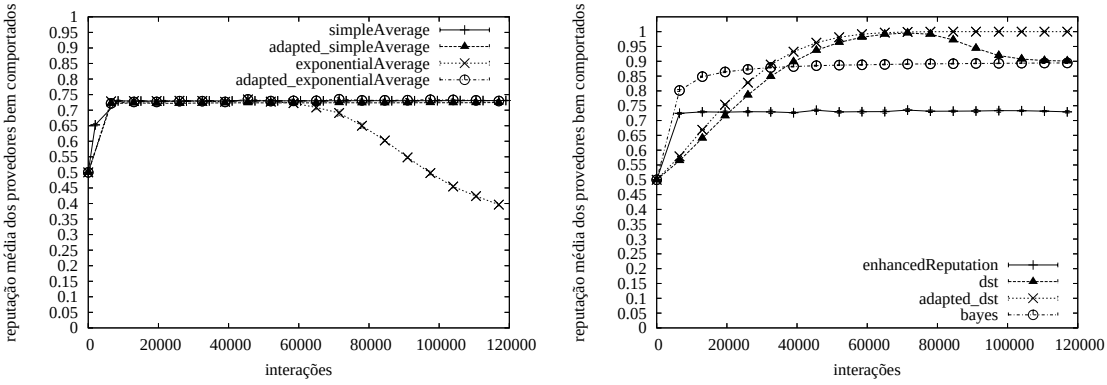
Figura 5.5: Variação de ρ (H = 10) - Percentual de Decisões Acertadas

Este cenário também foi simulado considerando que os métodos que usam históricos guardam 100 avaliações recentes. As figuras 5.6, 5.7, 5.8 e 5.9 mostram os resultados.



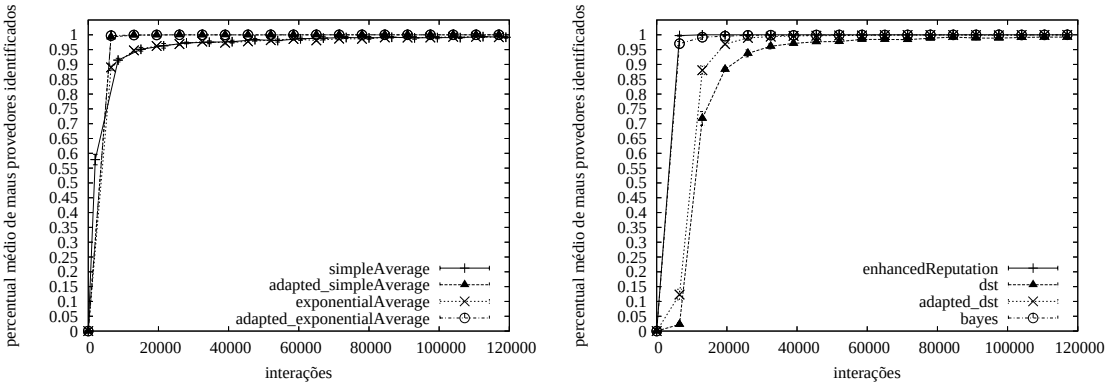
(a) (b)

Figura 5.6: H = 100 - Reputação Média dos Provedores Mal Comportados



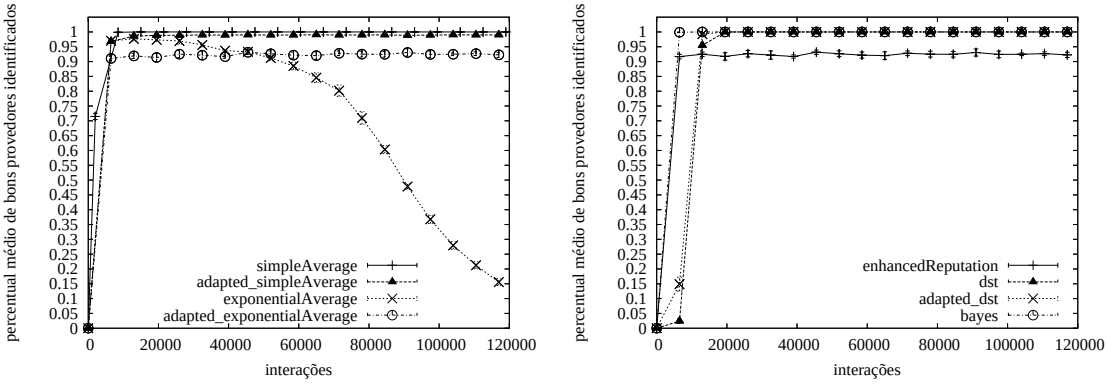
(a) (b)

Figura 5.7: H = 100 - Reputação Média dos Provedores Bem Comportados



(a) (b)

Figura 5.8: H = 100 - Percentual Médio de Maus Provedores Identificados



(a) (b)

Figura 5.9: H = 100 - Percentual Médio de Bons Provedores Identificados

Foi observada, na figura 5.8(a), uma sutil perda de velocidade de convergência do método de média simples. Como foi visto na seção 3.4.1, este método faz uso da equação 3.3 e, segundo esta equação, quanto maior o tamanho máximo H dos históricos, ou seja, quanto mais interações forem necessárias para preenchê-los, mais lento será o crescimento do peso das informações de primeira mão ($\eta = h/H$).

Assim, quando um dado cliente possui um número reduzido de interações com um provedor, o valor de reputação que irá calcular dependerá quase que totalmente das informações de segunda mão que ele receber. No início da simulação, quando muitas testemunhas possuem pouca ou nenhuma experiência para compartilhar, este aspecto acaba causando esta pequena diferença de convergência.

Considere, por exemplo, um dado cliente, que possui 5 avaliações em seu histórico a respeito de um dado provedor. Com um histórico de tamanho 100, este cliente associa um peso de apenas 0.05 às suas informações de primeira mão, mas se estivesse usando um histórico de tamanho 10 já estaria associando a elas um peso de 0.5. Numa situação como esta, se as testemunhas consultadas por este cliente não fornecerem informações de segunda mão conclusivas, a reputação final calculada com histórico de 10 talvez proporcionasse alguma indicação a respeito do comportamento do provedor enquanto que isso não seria conseguido com o histórico de tamanho 100.

É importante frisar que a perda de velocidade de convergência do método de média simples observada nos gráficos é bem pequena, pois logo os clientes da rede começam a interagir e se tornam capazes de fornecer testemunhos fora da zona de valores neutros.

O método de média simples adaptado não apresentou este efeito de perda na velocidade de convergência com o aumento no tamanho dos históricos. Neste método, o peso associado às informações de primeira mão é constante e igual a 0.5, ou seja, em nenhum momento assume um valor menor que o peso das informações de segunda mão.

Com relação à identificação de provedores bem comportados, a figura 5.9(a) mostrou que o aumento do tamanho do histórico teve uma influência positiva no método de média simples. A reputação calculada, levando em conta um número maior de avaliações e utilizando por mais tempo as informações de segunda mão, evitou que provedores bem comportados que cometessem poucos erros consecutivos tivessem suas reputações reduzidas abaixo do valor indicativo de bom comportamento.

Com relação ao método exponencial, a maior quantidade de avaliações guardadas nos

históricos reduziram um pouco a rapidez de convergência do método. Além disso, um histórico maior faz com que o método utilize por mais tempo as informações de segunda mão. Todos estes fatores explicam a melhora no desempenho deste método, notada pelas quedas mais tardias na reputação média dos provedores bem comportados (figura 5.7(a)) e no percentual de provedores bem comportados identificados (figura 5.9(a)).

Já no que diz respeito aos métodos que usam a teoria de Dempster-Shafer, em ambos os métodos, as crenças calculadas por um cliente para um determinado provedor a partir das avaliações armazenadas em histórico usam as equações 3.12 e 3.13. Observando estas equações, conclui-se que a crença $m(T)$ é o percentual de avaliações presentes no histórico que estão acima do valor limite indicativo de bom comportamento Ω. De maneira análoga, $m(notT)$ é o percentual de avaliações cujos valores estão abaixo de um valor limite indicativo de mau comportamento ω.

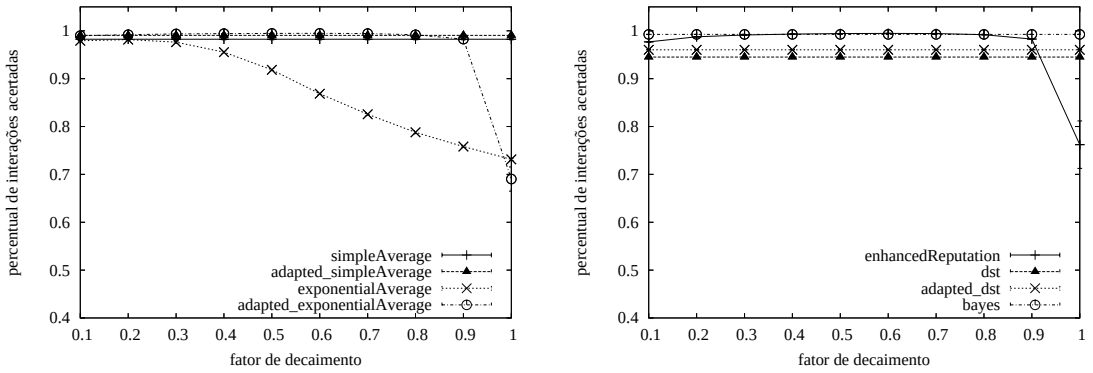
Quanto maior o tamanho do histórico, mais lentamente crescerá a crença em alguma das hipóteses, pois mais interações serão necessárias para fazer com que o percentual de avaliações acima de Ω ou abaixo de ω aumente e faça com que $m(T)$ ou $m(notT)$ assuma um valor significativo, reduzindo então a incerteza $m(T, notT)$. A redução mais lenta no valor da incerteza faz com que os valores de reputação, calculados através da equação 3.28, também demorem mais a crescer ou a reduzir acusando o bom ou mau comportamento dos provedores

Este aspecto é notado pela descida mais lenta das curvas de reputação média dos provedores mal comportados e pela subida mais lenta das curvas de reputação média dos provedores bem comportados, mostradas respectivamente pelas figuras 5.6(b) e 5.7(b). As figuras 5.8(b) e 5.9(b) também apontam o mesmo efeito demonstrando uma maior demora na identificação de provedores mal e bem comportados pelos métodos dst e dst adaptado.

O efeito da variação do fator de decaimento também foi estudado para este tamanho de histórico. A figura 5.10 mostra que a adoção do maior tamanho de histórico melhorou o desempenho do método exponencial para todos os valores de fator de decaimento testados. Os demais métodos que usam esta constante não foram afetados significativamente.

Quanto aos métodos que não usam o fator de decaimento, foram mantidos na figura para que seus percentuais de decisões acertadas fossem comparados com a configuração anterior, que usou um histórico menor. É perceptível a perda de desempenho dos métodos

que usam a teoria de Dempster-Shafer e uma queda bem pequena no percentual de acertos do método de média simples, resultados esperados pelos motivos expostos acima.

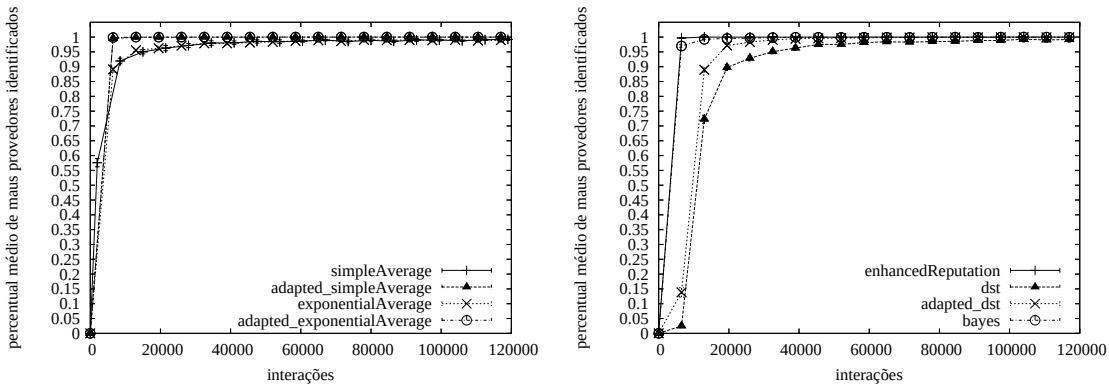


(a) (b)

Figura 5.10: Variação de ρ (H = 100) - Percentual de Decisões Acertadas

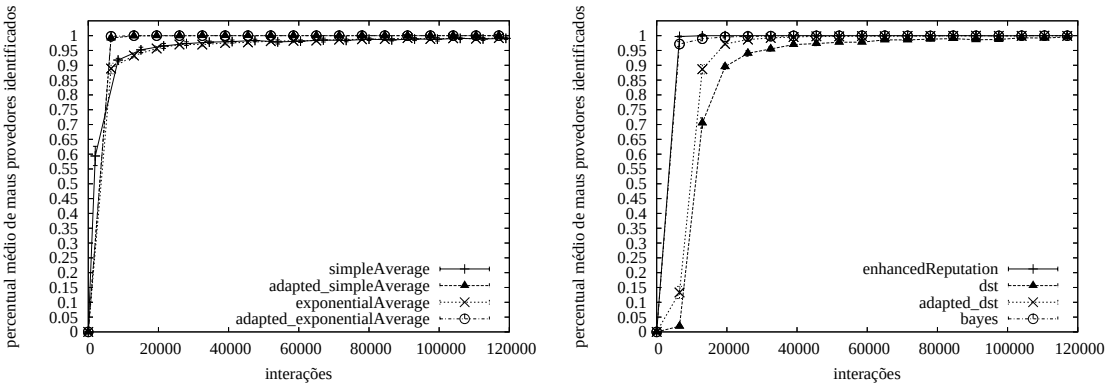
Como já foi citado, os testes apresentados até este momento para este cenário consideraram que os métodos que usam a equação 3.4 no cálculo final da reputação atribuíram o valor 0.5 ao peso α. Entretanto, alguns artigos sugerem que as informações de primeira mão, por serem consideradas mais confiáveis, devem ter maior peso.

Os gráficos a seguir mostram os resultados obtidos nas simulações que consideraram $\alpha = 0.6$ e $\alpha = 0.7$. Para os métodos que usam históricos, foi configurado o tamanho 100. As figuras 5.11 e 5.12 mostram que o aumento desta constante não afetou em nada a identificação dos provedores mal comportados. Já as figuras 5.13 e 5.14 mostram que o aumento de α causou prejuízo na identificação de provedores bem comportados.



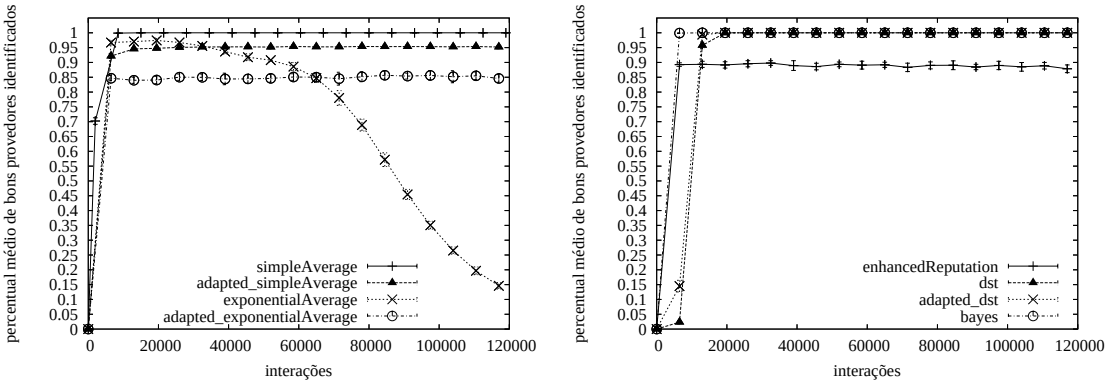
(a) (b)

Figura 5.11: α = 0.6 e H = 100 - Percentual Médio de Maus Provedores Identificados



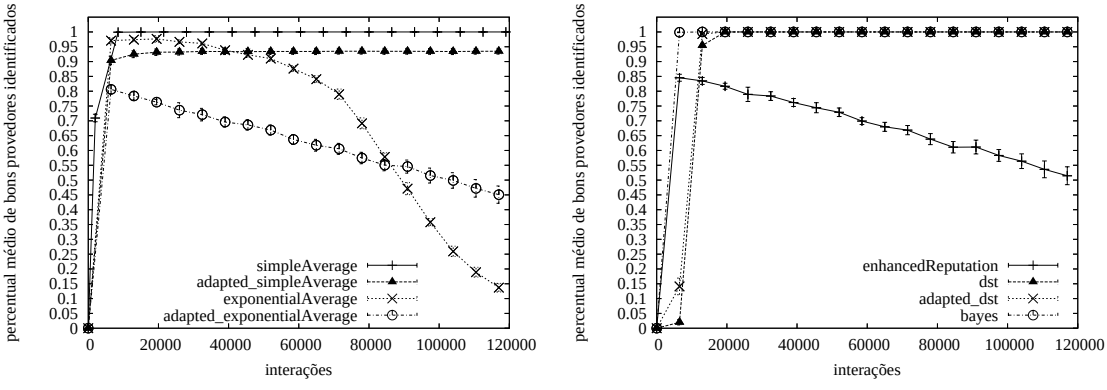
(a) (b)

Figura 5.12: α = 0.7 e H = 100 - Percentual Médio de Maus Provedores Identificados



(a) (b)

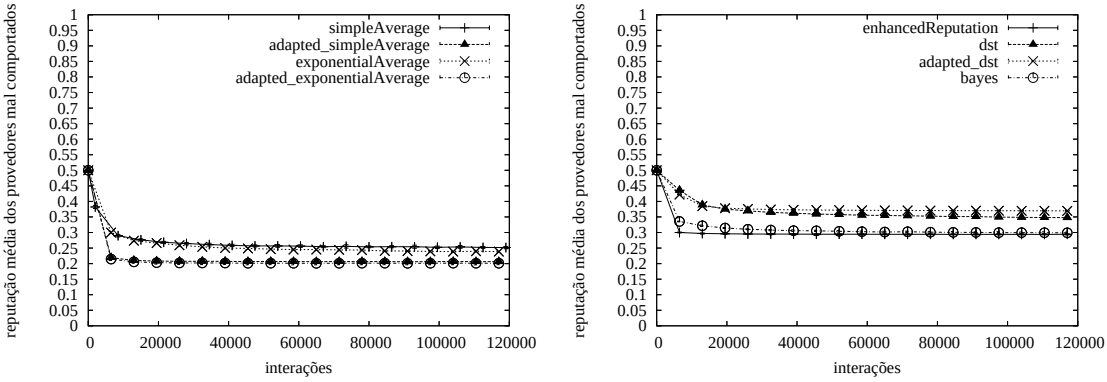
Figura 5.13: α = 0.6 e H = 100 - Percentual Médio de Bons Provedores Identificados



(a) (b)

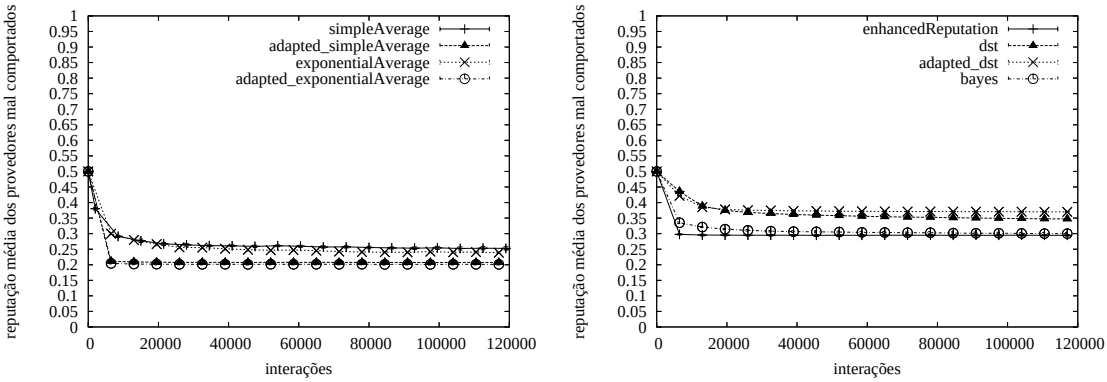
Figura 5.14: α = 0.7 e H = 100 - Percentual Médio de Bons Provedores Identificados

Estes efeitos são comprovados pelos gráficos das figuras 5.15 e 5.16, que mostram inalteradas as curvas de reputação média dos provedores mal comportados, e pelos gráficos das figuras 5.17 e 5.18, que mostram queda nos valores de reputações calculadas para os provedores bem comportados pelos métodos que usam a equação 3.4.



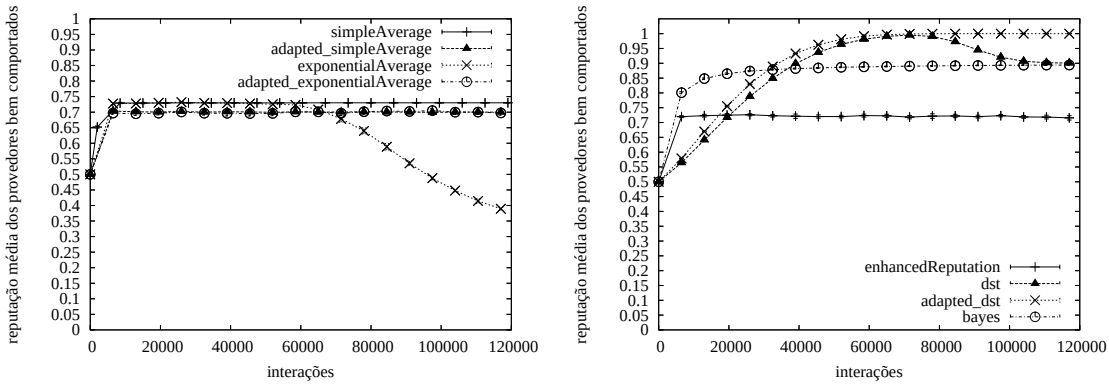
(a) (b)

Figura 5.15: α = 0.6 e H = 100 - Reputação Média dos Provedores Mal Comportados



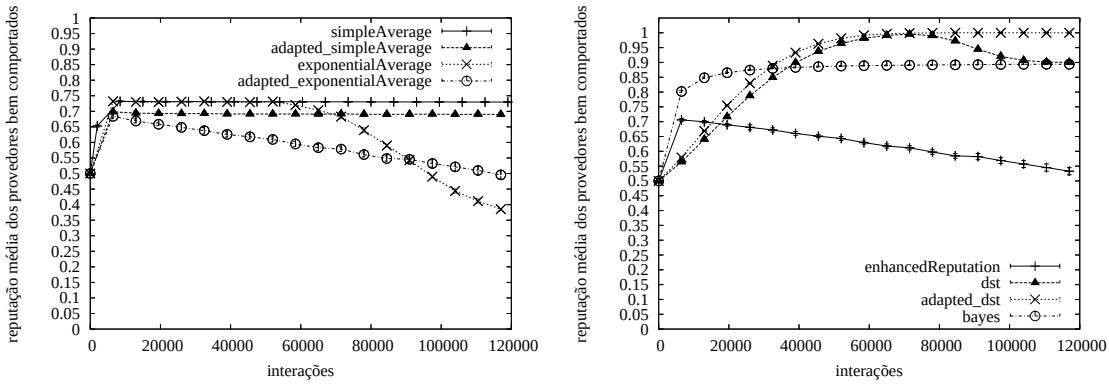
(a) (b)

Figura 5.16: α = 0.7 e H = 100 - Reputação Média dos Provedores Mal Comportados



(a) (b)

Figura 5.17: α = 0.6 e H = 100 - Reputação Média dos Provedores Bem Comportados

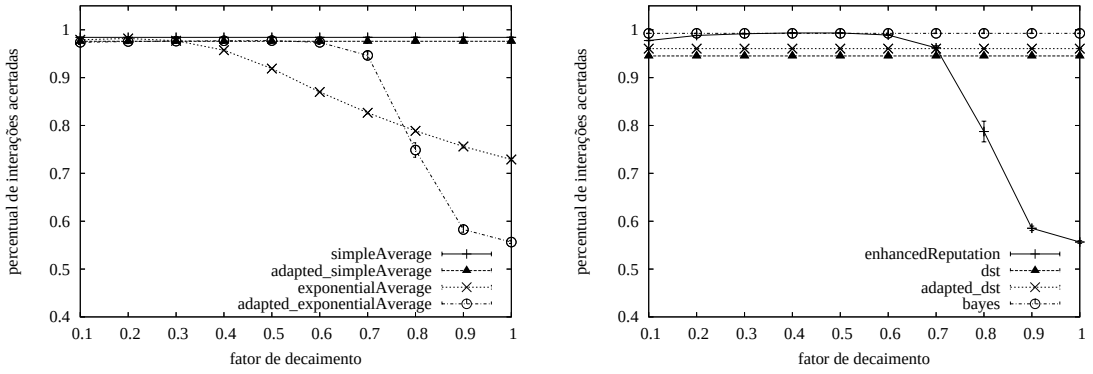


(a) (b)

Figura 5.18: α = 0.7 e H = 100 - Reputação Média dos Provedores Bem Comportados

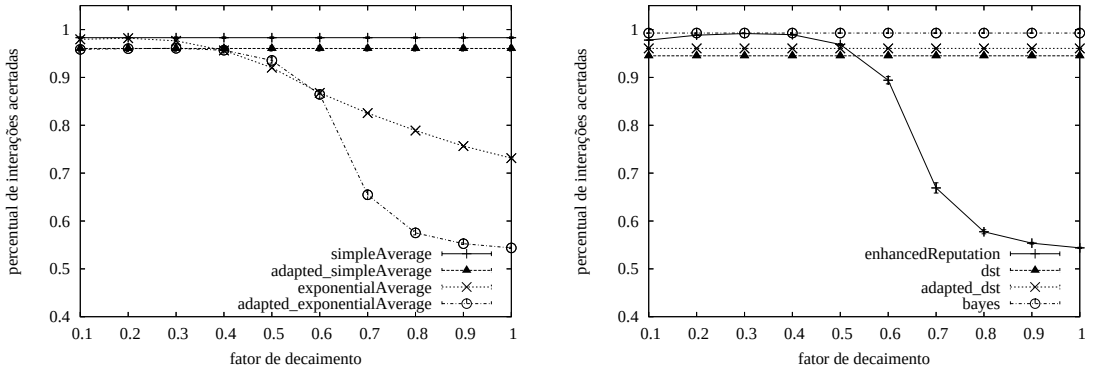
O aumento no peso das informações de primeira mão tornou o método exponencial adaptado e o método exponencial sem histórico sensíveis aos efeitos da convergência exagerada de suas agregações das informações de primeira mão. O método de média simples adaptado sofreu uma baixa pouco significativa na identificação de provedores bem comportados, visto que este método não usa o fator de decaimento e, portanto, não sofre os mesmos efeitos de convergência que os exponenciais.

As figuras 5.19 e 5.20 apresentam os percentuais de acertos atingidos pelos métodos quando o fator de decaimento é variado nas simulações que definem $\alpha = 0.6$ e $\alpha = 0.7$.



(a) (b)

Figura 5.19: Variação de ρ (α = 0.6) - Percentual de Decisões Acertadas



(a) (b)

Figura 5.20: Variação de ρ (α = 0.7)- Percentual de Decisões Acertadas

Com o aumento do peso das informações de primeira mão, os métodos exponenciais se tornaram mais sensíveis aos efeitos da maior convergência propiciada pelos maiores valores adotados para o fator de decaimento. Além disso, é notável que, para ambos valores de α testados, a queda de desempenho causada pelo aumento no fator de decaimento leva o método exponencial adaptado e o método exponencial sem histórico a percentuais de acertos menores que os atingidos pelo método exponencial, que até o momento apresentava os piores resultados.

Isso acontece porque o métodos exponenciais começam a simulação com um peso 1 para as informações de segunda mão e este peso vai sendo reduzido ao longo das interações até assumir o valor 0. Já nos outros dois métodos exponenciais, o peso das informações de primeira mão, quando configurado num alto valor, já inicia a simulação

neste valor, expondo estes métodos por mais tempo aos efeitos da convergência exagerada do cálculo de agregação das informações de primeira mão.

Até aqui se observou um bom desempenho atingido pelo método Bayesiano, que não usa histórico e nem o peso α no cálculo dos valores de reputação. Na seção 3.4.8 foi exposto que o método de Bayes pode fazer uso da constante u, que funciona como uma espécie de fator de decaimento (equações 3.16 e 3.17) no momento da atualização das informações de primeira mão. Sendo assim, a figura 5.21 mostra o percentual de acertos deste método para diversos valores desta constante. Como pode ser observado, neste cenário, não houve influência significativa do uso desta constante u.

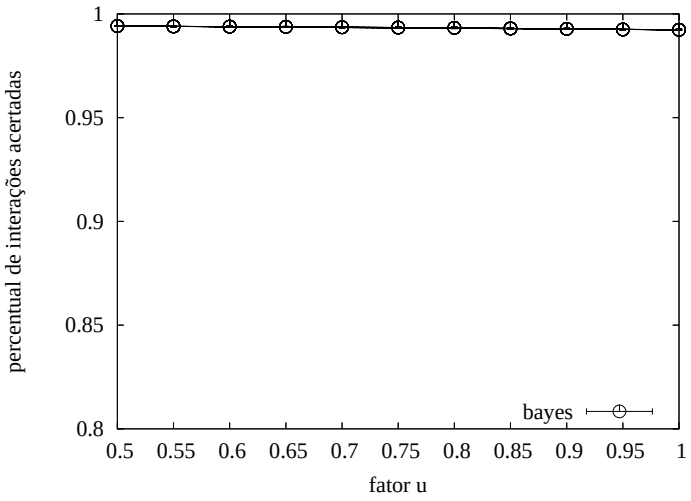


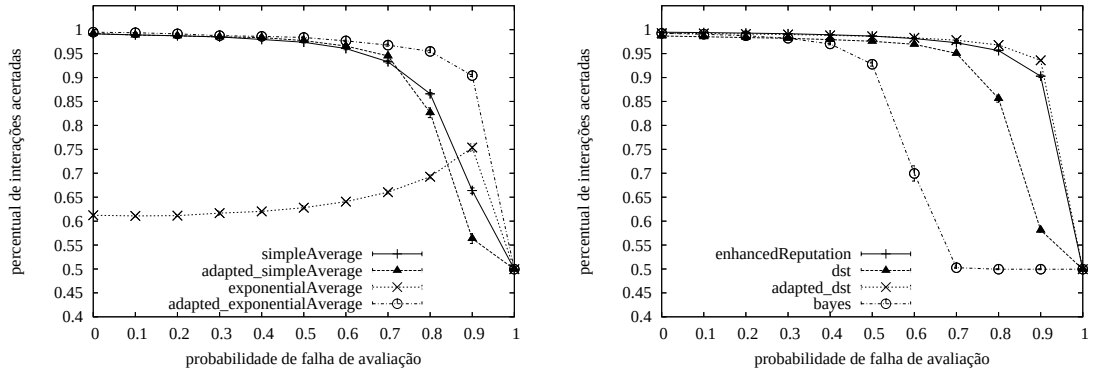
Figura 5.21: Variação de u - Percentual de Decisões Acertadas

5.2 Cenário 2 - Possibilidade de Falha de Avaliação

O cenário dois mantém muitas das características do Cenário 1. Metade dos provedores são mal comportados, não há provedores que aplicam o ataque da mudança repentina de comportamento, as testemunhas são escolhidas aleatoriamente durante a geração de cenário e não há clientes aplicando o ataque do testemunho mentiroso. Entretanto, para as simulações executadas neste cenário, foi configurada a probabilidade de falha na avaliação, ou seja, um dado cliente poderá, ao final da interação, não conseguir analisar de maneira conclusiva o comportamento do provedor (seção 4.2).

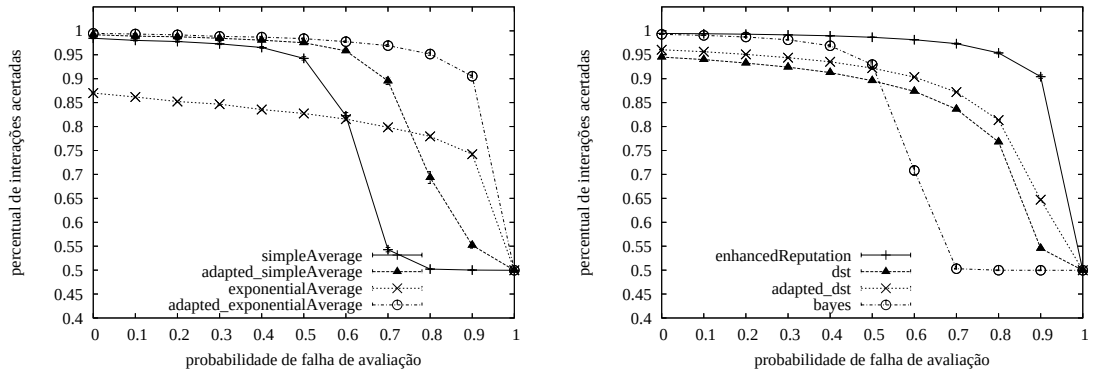
Os gráficos das figuras 5.22 e 5.23 apresentam os percentuais de acertos de cada método para os vários valores de probabilidade de falha de avaliação testados. Os gráficos

da figura 5.22 resultam de simulações que consideraram 10 avaliações para o tamanho máximo dos históricos. Nas simulações da figura 5.23, o tamanho dos históricos definido foi 100. No que se refere aos métodos que usam a equação 3.4 no cálculo final da reputação, o peso α foi configurado no valor 0.5.



(a) (b)

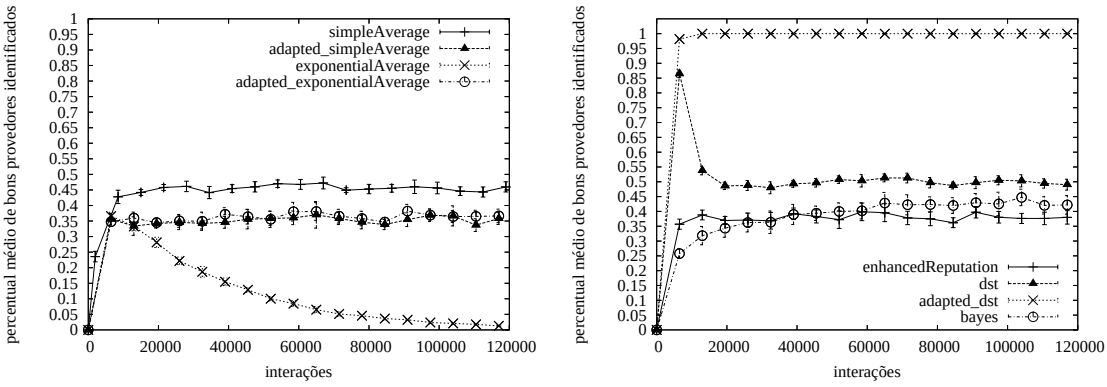
Figura 5.22: Variação de FALHA_AVALIACAO (H = 10) - Percentual de Acertos



(a) (b)

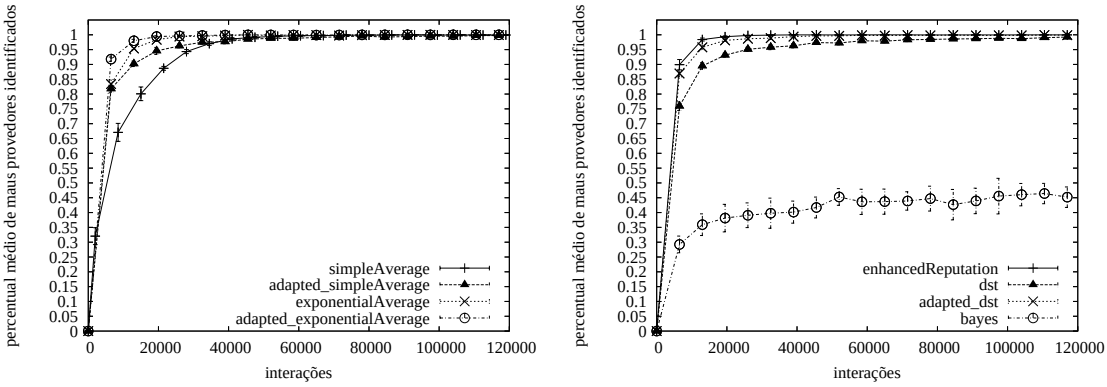
Figura 5.23: Variação de FALHA_AVALIACAO (H = 100) - Percentual de Acertos

Para auxiliar na análise destes resultados, recorre-se ainda aos gráficos das figuras 5.24, 5.25, 5.26 e 5.27 que mostram os percentuais de provedores bem e mal comportados identificados para os tamanhos de histórico 10 e 100 quando a probabilidade de falha na avaliação foi considerada 0.6.



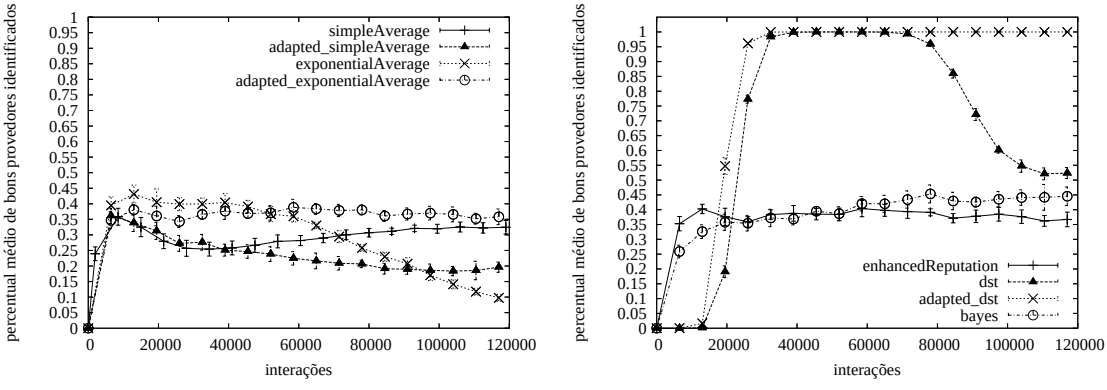
(a) (b)

Figura 5.24: H = 10 - Percentual Médio de Bons Provedores Identificados



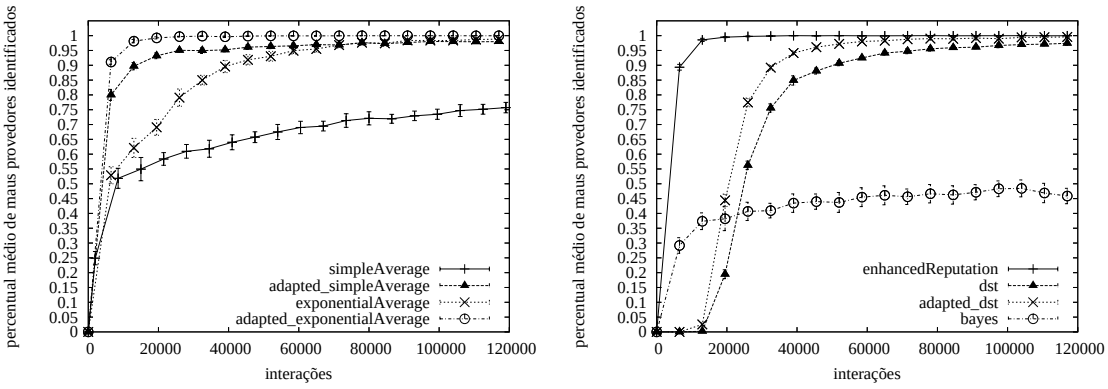
(a) (b)

Figura 5.25: H = 10 - Percentual Médio de Maus Provedores Identificados



(a) (b)

Figura 5.26: H = 100 - Percentual Médio de Bons Provedores Identificados



(a) (b)

Figura 5.27: H = 100 - Percentual Médio de Maus Provedores Identificados

As figuras 5.22(a) e 5.23(a) mostraram que os métodos de média simples apresentaram quedas de desempenho mais acentuadas quando o tamanho de histórico considerado foi 100. Quanto menos avaliações consideradas no cálculo de primeira mão (equação 3.1), menos interações sem falhas de avaliação serão suficientes para que o valor resultante seja conclusivo, ou seja, indicativo de bom ou mau comportamento. Comprovando este efeito, as figuras 5.26(a) e 5.27(a) mostraram menores percentuais de detecção de provedores bem e mal comportados pelos métodos de média simples que as figuras 5.24(a) e 5.25(a).

A perda da capacidade de identificar provedores mal comportados é o principal causador da queda no percentual de acertos destes métodos. Quanto mais avaliações falhas, mais as reputações dos provedores mal comportados se aproximarão de valores neutros, que não impedirão os clientes de interagir com eles. A perda da capacidade de identificar provedores bem comportados já não causa tanto prejuízo, pois a aproximação das reputações destes provedores para valores neutros não fará com que os clientes deixem de interagir com eles.

Ainda a respeito dos métodos de média simples, quando o histórico foi configurado para 100, foi possível perceber que o método de média simples original teve seu desempenho mais afetado pelo aumento da probabilidade de falha de avaliação do que o método adaptado. A utilização da equação 3.3 faz com que um tamanho grande de histórico torne mais lento o crescimento do peso dado às informações de primeira mão. Enquanto este peso é muito baixo, para que um cliente consiga identificar o comportamento de um provedor, ele depende de informações de segunda mão conclusivas, mais difíceis de conseguir quanto maior for o valor da probabilidade de falha na avaliação.

Com relação aos métodos que usam fator de decaimento, o valor adotado para esta constante nas simulações que deram origem a estes gráficos foi 0.6. A figura 5.22(a) mostrou que o método exponencial foi o único a sofrer um aumento de desempenho com o aumento da probabilidade de falha de avaliação. Conforme foi visto no estudo do Cenário 1, quando um pequeno tamanho de histórico é utilizado, este método sofre muito por conta de sua velocidade de convergência exagerada, que é causadora de maus julgamentos de provedores bem comportados.

Com o aumento da probabilidade de falha na avaliação, maiores são as chances dos clientes deixarem de detectar as interações falhas dos provedores bem comportados. A figura 5.24(a) mostrou que este método não ganha capacidade de detectar provedores bem comportados, entretanto a aproximação de suas reputações de valores neutros, evita que eles sejam considerados mal comportados.

Como já era esperado, por causa dos resultados estudados no Cenário 1, a figura 5.23(a) mostrou que o método exponencial apresentou um melhor desempenho quando o tamanho de histórico foi 100. Pôde-se até observar uma queda no percentual de acertos com o aumento na probabilidade de falha na avaliação.

Embora a figura 5.26(a) tenha apontado para uma queda mais lenta da capacidade deste método de identificar provedores bem comportados, consequência da convergência mais lenta trazida pelo uso do maior histórico, a comparação entre as figuras 5.27(a) e 5.25(a) mostrou uma redução bastante significativa em sua capacidade de identificar provedores mal comportados.

O uso da equação 3.3 no cálculo final da reputação faz com que maiores históricos levem este método a demorar mais interações para associar um peso maior às informações de primeira mão. Assim, o cálculo da reputação depende, por mais tempo, de informações de segunda mão conclusivas, mais difíceis de se conseguir quanto maior a probabilidade de falha na avaliação. Com isso, as reputações calculadas se aproximam de valores neutros e o aumento de provedores mal comportados não identificados provoca a queda no percentual de percentual, mostrada pela figura 5.23(a).

A comparação entre as figuras 5.27(a) e 5.25(a) mostrou ainda que, praticamente, não existiu diferença entre os percentuais de provedores mal comportados identificados pelo método exponencial adaptado com históricos de tamanho 100 e 10. O uso de um peso constante para as informações de segunda mão, que nunca supera o peso associado às

experiências próprias, faz com que este método aproveite bem os efeitos da utilização do fator de decaimento e possa garantir bons índices de detecção dos provedores mal comportados.

A figura 5.22(b) mostrou que o método exponencial que não usa histórico tem um desempenho praticamente igual ao do método exponencial adaptado. A utilização da equação 3.4 garante a este método uma boa capacidade de detecção dos provedores mal comportados (figura 5.25(b)), que lhe proporcionou bons percentuais de decisões acertadas.

Com relação a detecção de provedores bem comportados, as figuras 5.24 e 5.26 mostraram que todos os métodos exponenciais estudados (métodos exponencial, exponencial adaptado e exponencial sem histórico) apresentaram dificuldades. Isso ocorre porque, quando um cliente identifica um provedor bem comportado, volta a fazer novas interações com ele. Se estas interações resultarem em avaliações falhas, seu valor final de reputação será atualizado e reduzido, aproximando-se novamente de valores neutros.

Este aspecto, entretanto, não chega representar prejuízo para os métodos, pois os clientes se mantêm requisitando recursos/serviços destes provedores, o que não causará queda no percentual de decisões acertadas.

Quanto aos mecanismos que usam a teoria de Dempster-Shafer, merecem uma especial atenção, tendo em vista que uma de suas das principais características é o fato deste método matemático possuir uma representação para incerteza. Este diferencial trazido pelos mecanismos que fazem uso da teoria de Dempster-Shafer sugere que seus desempenhos deveriam ser superiores ao dos demais métodos neste cenário. Observando o gráfico da figura 5.22(b), verifica-se que o desempenho alcançado pelo método dst original foi bem semelhante aos alcançados pelos métodos que usam média simples quando o tamanho de histórico adotado foi 10.

O método dst pára de usar as informações de segunda mão quando os históricos são preenchidos. As crenças, calculadas pelas equações 3.12 e 3.13, passam a ser usadas diretamente pela equação 3.28 no cálculo final de reputação e a regra de combinação de Dempster-Shafer passa a não ser mais utilizada. Conforme mostra a figura 5.25(b), os clientes apresentaram capacidade de identificar os provedores mal comportados de maneira a não interagirem com eles.

O método dst adaptado obteve, entretanto, o melhor desempenho dentre todos os

métodos estudados para todos os valores de probabilidade de falha de avaliação testados. Esse método usa as informações de segunda mão durante toda a simulação, agregando-as com as informações de primeira mão através da regra de combinação de Dempster-Shafer (equações 3.9, 3.10 e 3.11). O resultado desta agregação são as crenças consideradas no cálculo final de reputação feito pela equação 3.28.

A regra de combinação de Dempster-Shafer, que trabalha de maneira explícita com a incerteza no momento da agregação das crenças, permitiu aos clientes não só identificarem os provedores mal comportados (figura 5.25(b)) como também manterem suas capacidades de identificação dos provedores bem comportados (figura 5.24(b)), o que mostra que a utilização desta regra neste cenário realmente proporcionou a este mecanismo um diferencial em relação aos que fazem uso da teoria tradicional de probabilidade.

A figura 5.23 mostrou mais uma vez que ambos os métodos que usam a teoria de Dempster-Shafer são bastante afetados pelo aumento no tamanho do histórico, conforme já havia sido discutido no estudo do Cenário 1. Ainda assim, o método adaptado continuou apresentando um melhor desempenho, em comparação com o método dst original, para todos os valores de probabilidade de falha na avaliação testados.

Quanto ao método Bayesiano, o gráfico da figura 5.22(b) mostrou que o percentual de acertos deste método sofreu uma queda brusca antes de todos os outros. A figura 5.25(b) mostrou a dificuldade deste método em manter a capacidade dos clientes identificarem os provedores mal comportados. Foi o pior percentual de identificação.

No método de Bayes, quando um cliente não consegue avaliar um provedor, s e f, das equações 3.14 e 3.15, assumem o valor 1. Sendo assim, quando a probabilidade de falha é alta, com o passar das interações, os valores de α_{ij} e β_{ij} crescem. Isso torna cada vez mais difícil para um cliente que esteja usando este método aumentar o valor de β_{ij} de maneira que o cálculo da reputação θ, feito pela equação 3.25, tenda a valores conclusivos.

Conforme mostra a figura 5.28, o desempenho do método Bayesiano sofre melhora com a configuração da constante u com valores menores que 1 (equações 3.16 e 3.17). Entretanto, este método continua sendo bastante afetado e sua curva de percentual de interações acertadas só se aproxima das curvas dos demais métodos quando o valor de u é configurado com o valor zero.

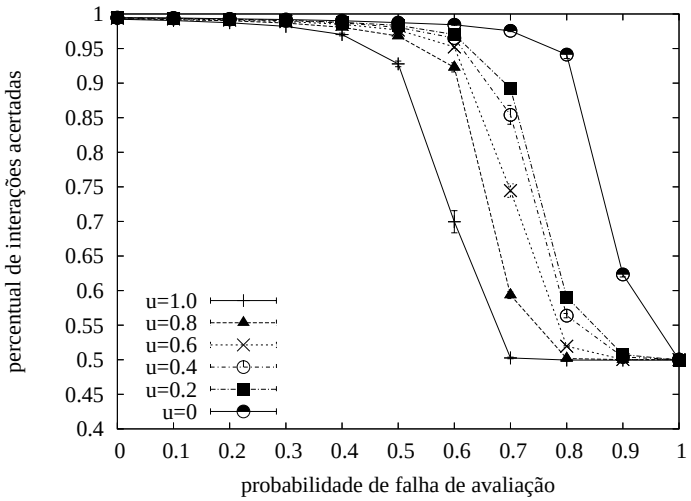
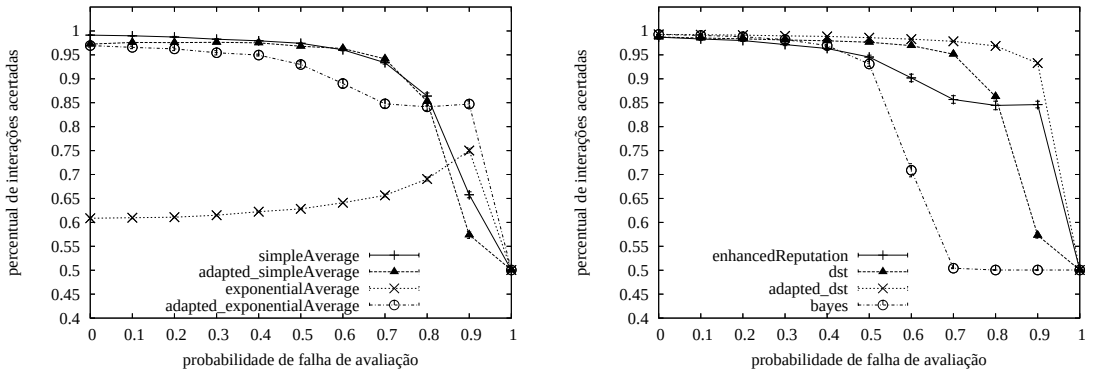


Figura 5.28: Variação de u - Percentual de Decisões Acertadas

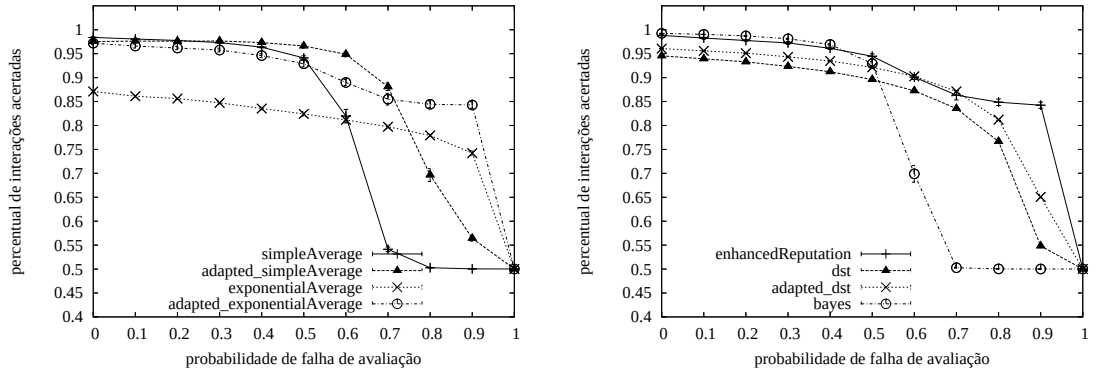
As simulações de todos os métodos foram repetidas neste mesmo cenário considerando que um maior peso α foi atribuído às informações de primeira mão pelos métodos que fazem uso da equação 3.4 no cálculo final da reputação. As figuras 5.29 e 5.30 mostram que o método de média simples adaptado sofreu uma mudança de comportamento pouco significativa.

O método exponencial adaptado e o método exponencial que não usa histórico tiveram seus desempenhos piorados. Estes resultados confirmam o que já havia sido estudado no Cenário 1. Quanto maior o peso associado às informações de primeira mão, maior serão os efeitos dos maus julgamentos de provedores bem comportados provocados pela convergência acelerada na agregação das informações de primeira mão destes métodos.



(a) (b)

Figura 5.29: Variação de FALHA_AVALIACAO H = 10 α = 0.6 - Percentual de Acertos

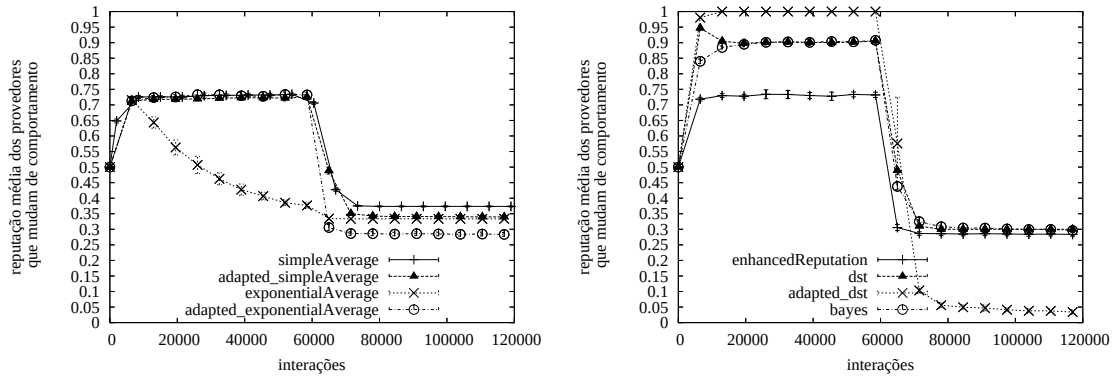


(a) (b)

Figura 5.30: Variação de FALHA_AVALIACAO H=100 e α = 0.6 - Percentual de Acertos

5.3 Cenário 3 - Mudança Repentina de Comportamento

Tal como no Cenário 1, no Cenário 3, as testemunhas são escolhidas aleatoriamente durante a fase de geração de cenário, não há clientes aplicando o ataque do testemunho mentiroso, não existe probabilidade de falha na avaliação dos clientes. Neste cenário, entretanto, está presente um provedor aplicando o ataque da mudança repentina de comportamento (seção 3.6.2).



(a) (b)

Figura 5.31: H = 10 - Reputação Média do Provedor que Mudou de Comportamento

Os gráficos da figura 5.31 apresentam as curvas de reputação média do provedor que está praticando o ataque. As simulações que deram origem a estes gráficos consideraram que os métodos que fazem uso de históricos adotaram tamanho 10, que os que usam fator

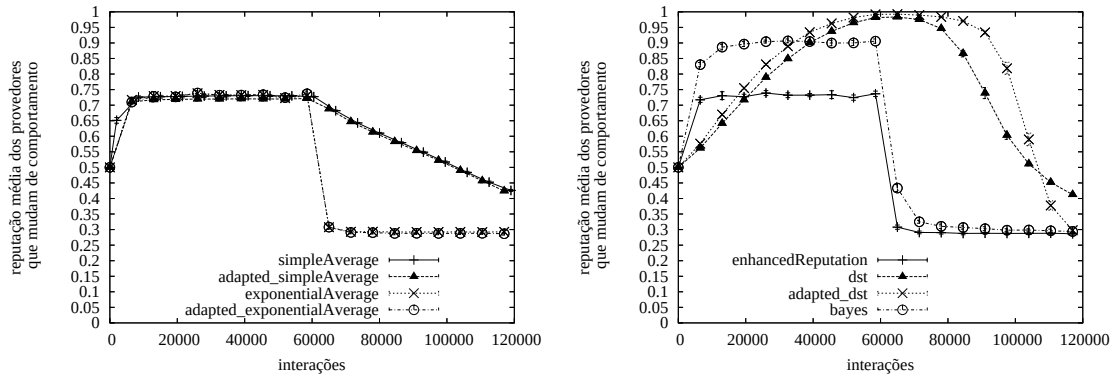
de decaimento consideraram o valor de 0.6 para esta constante, que o método Bayesiano foi foi configurado com $u = 0.8$ e que os métodos que usam a equação 3.4 no cálculo final da reputação foram configurados para associar ao peso α o valor 0.5.

O método exponencial, por causa de sua convergência exageradamente rápida, já associava ao provedor uma reputação muito baixa, antes mesmo dele se tornar mal comportado. O método exponencial adaptado e o método exponencial que não usa histórico têm desempenhos muito semelhantes. Ambos detectam a mudança de comportamento do provedor antes de todos os outros métodos, mostrando que o uso do fator de decaimento em conjunto com o uso constante das informações de segunda mão é uma vantagem neste cenário.

Os métodos que utilizam DST (o original e o adaptado) e o método Bayesiano, assim como os métodos que usam média simples, apesar de demorarem mais algumas interações para detectarem a mudança de comportamento do provedor, o fazem sem maiores problemas.

Os métodos que usam histórico foram testados neste mesmo cenário para o tamanho de histórico 100. A figura 5.32 mostra que os métodos que usam média simples não conseguiram detectar, até o fim da simulação, a mudança de comportamento. Para que essa detecção fosse possível, mais interações seriam necessárias, de forma que os grandes históricos que os clientes guardam deste provedor passassem a ter mais avaliações ruins e, assim a média resultasse em um valor indicativo de mau comportamento.

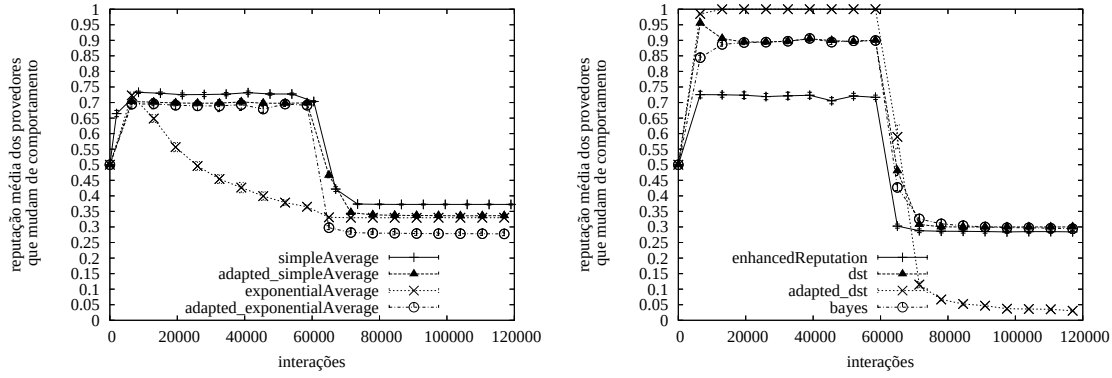
Já o método exponencial, como já era esperado, foi beneficiado pelo uso do maior histórico e teve seu comportamento aproximado dos demais métodos exponenciais. Os métodos que usam DST, como também já tinha sido constatado, são prejudicados pelo aumento do tamanho do histórico e, portanto, demoraram um número de interações bem maior para iniciarem a redução do valor de reputação associado ao provedor que mudou de comportamento.



(a) (b)

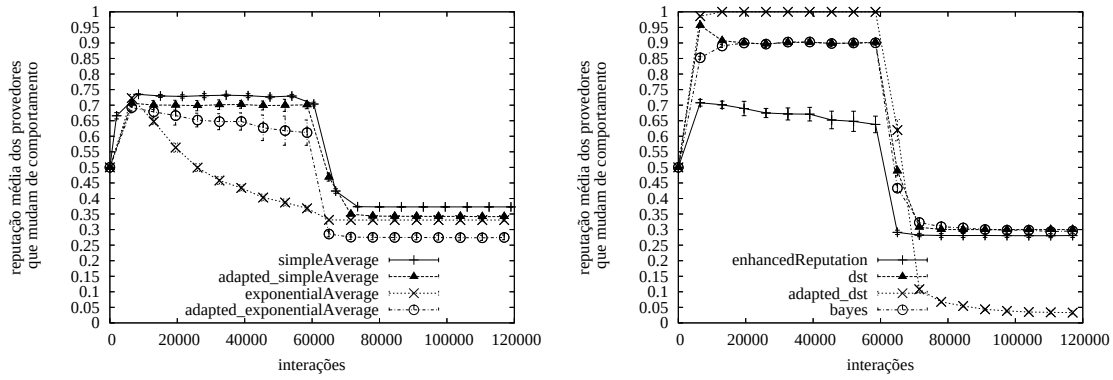
Figura 5.32: H = 100 - Reputação Média do Provedor que Mudou de Comportamento

Os métodos que usam a equação 3.4 no cálculo final da reputação foram testados também com α configurado para os valores 0.6 e 0.7. O tamanho do histórico para estas simulações foi considerado como 10.



(a) (b)

Figura 5.33: α = 0.6 - Reputação Média do Provedor que Mudou de Comportamento



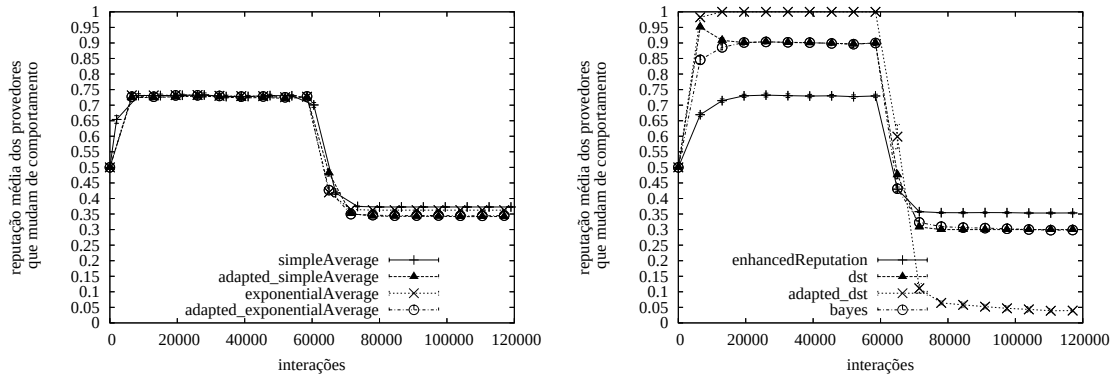
(a) (b)

Figura 5.34: α = 0.7 - Reputação Média do Provedor que Mudou de Comportamento

As figuras 5.33 e 5.34 mostraram que, na primeira metade da simulação, enquanto o provedor está se comportando bem, o aumento de α fez com a reputação média deste provedor fosse reduzida. Isso aconteceu principalmente nos métodos exponenciais, pois o efeito do fator de decaimento é acentuado pelo maior peso dado às informações de primeira mão. Entretanto, o número de interações passadas desde a mudança de comportamento do provedor até sua detecção como mal comportado não sofreu alteração significativa nos métodos que usam esta constante α.

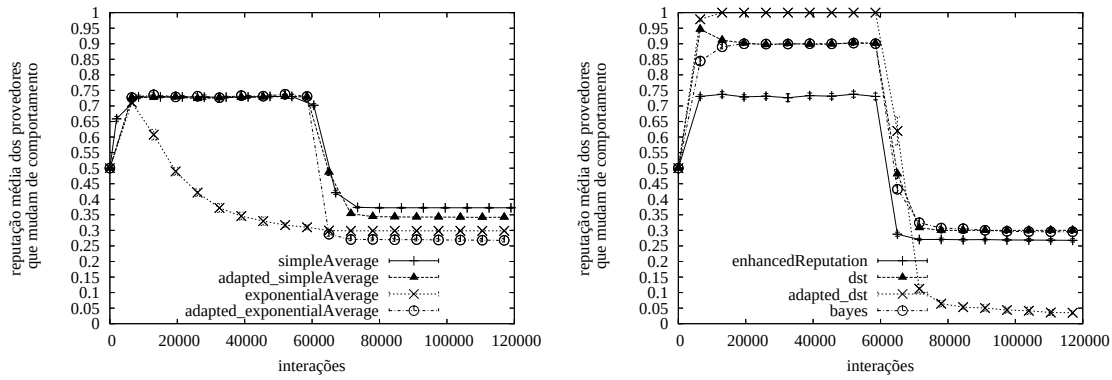
As simulações também foram repetidas para os valores de fator de decaimento 0.2 e 0.7. A figura 5.35 mostra que um valor muito reduzido de fator de decaimento aproxima a curva de reputação média do método exponencial das curvas conseguidas pelos métodos exponencial adaptado e exponencial sem histórico, resultado já esperado pelo estudo feito no cenário 1. Entretanto, a redução da convergência causada pela redução do fator de decaimento faz com que os métodos exponencial adaptado e sem histórico percam a vantagem que haviam obtido sobre os outros métodos, ou seja, eles passam a não detectarem a mudança de comportamento mais rápido que os demais.

Conforme esperado, a figura 5.36 mostra que o valor 0.7 de fator de decaimento manteve os métodos exponencial adaptado e sem histórico detectando a mudança de comportamento antes dos demais métodos, mas piorou o desempenho do método exponencial fazendo-o julgar mal o provedor analisado, na primeira metade da simulação, enquanto ele estava se comportando bem.



(a) (b)

Figura 5.35: $\rho = 0.2$ - Reputação Média do Provedor que Mudou de Comportamento



(a) (b)

Figura 5.36: $\rho = 0.7$ - Reputação Média do Provedor que Mudou de Comportamento

Quanto ao método de Bayes, a figura 5.37 mostra as curvas de reputação média do provedor conseguidas por este método para vários valores de u testados. Este gráfico mostra que este método não proporcionou aos clientes da rede a capacidade de detectar a mudança de comportamento do provedor quando u foi configurado com o valor 1.

Isso aconteceu porque, quando o provedor mudou de comportamento, no meio da simulação, os clientes já tinham tido muitas oportunidades de interagir com ele. Conseqüentemente, usando $u = 1$, os valores de α_{ij} associados por estes clientes a este provedor já tinham aumentado muito em relação aos valores de β_{ij} (equações 3.14 e 3.15). Nas interações que seguiram até o fim da simulação, os clientes começaram a incrementar β_{ij}, que ao fim da simulação atingiu um valor aproximadamente igual ao de α_{ij}, o que fez com que as reputações calculadas pelo método atingissem um valor em torno de 0.5.

Para que o método Bayesiano pudesse tornar os clientes capazes de detectar a mudança de comportamento do provedor neste cenário, foi necessário configurar a constante u com um valor diferente de 1 (equações 3.16 e 3.17). Isso proporcionou um decaimento dos valores de α_{ij} e β_{ij}, o que aumentou a velocidade de convergência do método. Quanto menor o valor de u, maior a convergência do método.

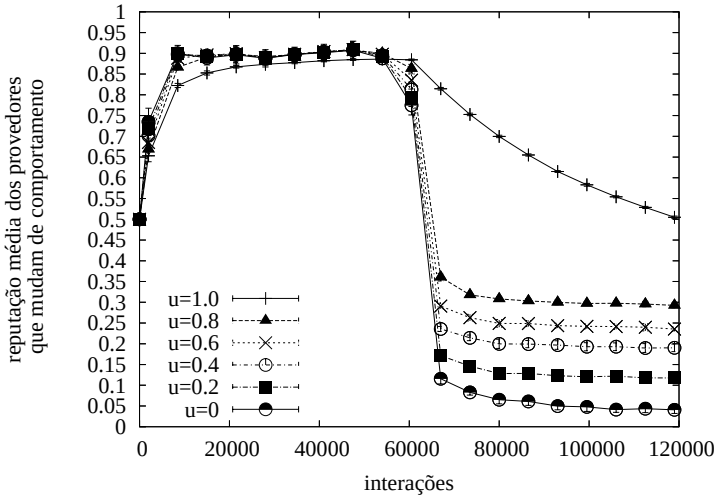


Figura 5.37: Variação de u-Reputação Média do Provedor que Mudou Comportamento

5.4 Cenário 4 - Testemunho Mentiroso

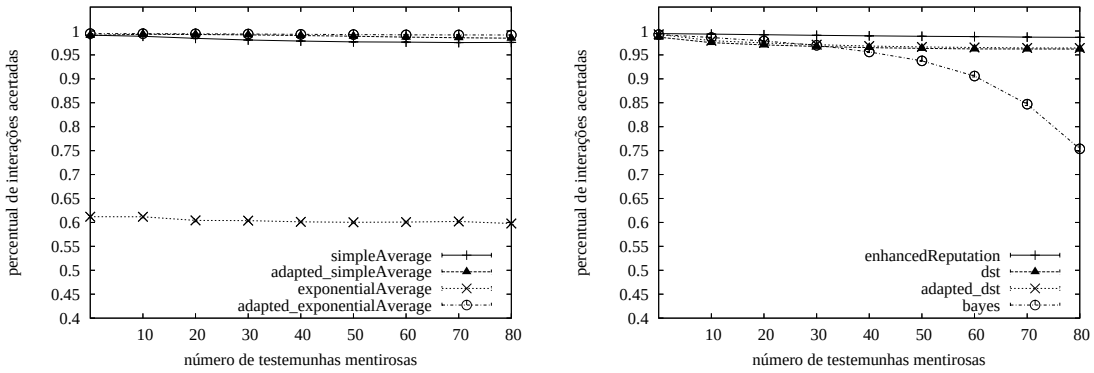
No Cenário 4, as testemunhas são escolhidas aleatoriamente durante a geração de cenário, não existe probabilidade de falha na avaliação dos clientes, não existem provedores aplicando o ataque da mudança repentina de comportamento, mas existem clientes aplicando o ataque do testemunho mentiroso [60].

O primeiro conjunto de configurações deste cenário considerou tamanho de histórico 10, fator de decaimento 0.6 e o peso α, usado pela equação 3.4, com valor 0.5. Foram testados os três modelos de mentira detalhados na seção 3.6.1, ou seja, o exagero negativo, o exagero positivo e a mentira complementar.

Na figura 5.38 é possível perceber que, nesta configuração, o modelo de exagero positivo não teve uma influência muito grande no desempenho da maior parte dos métodos. Com exceção do método de Bayes, que será analisado posteriormente nesta seção, os outros métodos, ainda que na presença de um número bem alto de testemunhas mentirosas, não apresentaram percentuais de acertos muito diferentes do que tinham quando não

existiam clientes aplicando este ataque na rede.

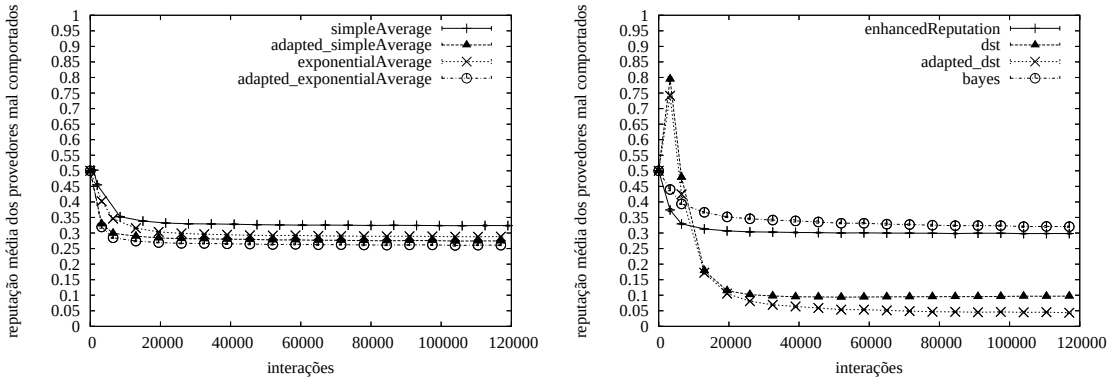
Isso ocorre porque, aplicando o ataque do exagero positivo, as testemunhas mentirosas podem fazer com que alguns clientes se enganem e decidam interagir com *peers* que são mal comportados, mas essas decisões erradas são evitadas quando estes clientes acumulam informações de primeira mão.



(a) (b)

Figura 5.38: Exagero Positivo - Percentual de Decisões Acertadas

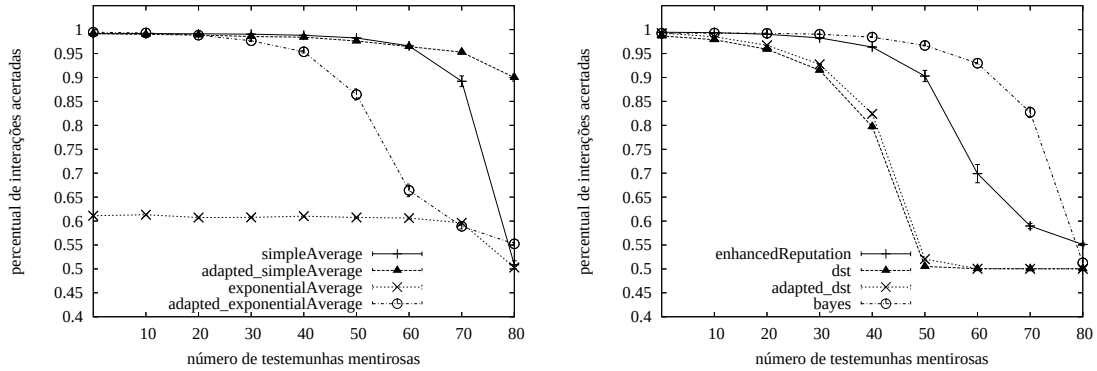
A figura 5.39 mostra como a reputação média dos provedores mal comportados foi afetada num ambiente que considerou a presença de 60 clientes aplicando o ataque do exagero positivo. Todos os métodos atingiram valores de reputação média abaixo do limiar indicativo de mau comportamento. Os métodos que usam a teoria de Dempster-Shafer sentiram os efeitos do ataque no início da simulação, entretanto esse problema foi sanado assim que os clientes acumularam experiências com os provedores mal comportados.



(a) (b)

Figura 5.39: Exagero Positivo - Reputação Média dos Provedores Mal Comportados

Já quando o ataque é o exagero negativo, o erro ao qual os clientes são induzidos é o de não interagir com provedores bem comportados. Deixando de interagir, os clientes que são vítimas do ataque não adquirem experiências e continuam usando as informações de segunda mão como principal fonte para suas tomadas de decisões, que continuam sendo influenciadas pelas mentiras. A figura 5.40 mostra a maior influência do exagero negativo.



(a) (b)

Figura 5.40: Exagero Negativo - Percentual de Decisões Acertadas

A figura 5.41 mostra como a reputação média dos provedores bem comportados foi afetada em cada método num ambiente que considerou a presença de 60 clientes aplicando o ataque do exagero negativo. O método de média simples é bastante afetado no início da simulação, pois os clientes, ainda sem experiências, associam peso 1 às informações de segunda mão (equação 3.3), se tornando bastante vulneráveis às testemunhas mentirosas. Somente quando os históricos estão cheios e os clientes passam a usar somente suas informações de primeira mão é que o método tem seu desempenho recuperado.

O mesmo acontece com o método exponencial, entretanto, este não se recupera da mesma maneira que o método de média simples, pois os maus julgamentos dos provedores bem comportados, causados por sua convergência exagerada, mantêm a reputação média destes *peers* abaixo do limiar indicativo de mau comportamento.

Quanto ao método exponencial adaptado e ao método exponencial sem histórico, também têm seus valores de reputação média reduzidos. Estes métodos usam a equação 3.4, ou seja, mantêm o mesmo peso associado às informações de segunda mão do início ao fim da simulação. O comportamento decrescente de seus valores de reputação média se devem ao fato destes métodos não poderem mais contar com informações confiáveis

das testemunhas, que amenizavam os efeitos da rápida convergência de seus cálculos de primeira mão.

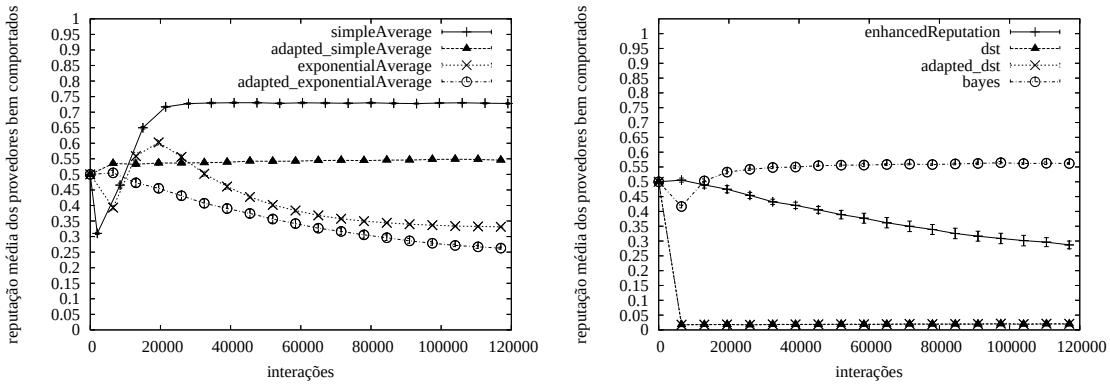
O método de média simples adaptado, que também usa a equação 3.4, consegue manter a reputação média dos provedores bem comportados num patamar neutro. Com isso, os clientes, mesmo não identificando estes provedores como bem comportados, também não os detectam como ruins e, sendo assim, não deixam de interagir com eles, mantendo o percentual de acertos alto.

Os mecanismos que fazem uso da teoria de Dempster-Shafer, cujas curvas de reputação média se sobrepõem na figura 5.41(b), são bastante afetados por este ataque. Isso se deve ao uso da regra de combinação de Dempster-Shafer na agregação das informações de segunda mão no início da simulação, enquanto os clientes possuem pouca experiência.

Para entender porque a utilização da regra de combinação causa este efeito, basta imaginar que um cliente honesto, que não tem experiência, informa as crenças $m(T) = 0$, $m(notT) = 0$ e $m(T, notT) = 1$. Enquanto isso, uma testemunha, igualmente sem experiência, porém mentirosa, informa $m(T) = 0$, $m(notT) = 0.4$ e $m(T, notT) = 0.6$. O resultado da combinação destas duas informações pela regra de combinação de Dempster-Shafer resulta nas crenças $m(T) = 0$, $m(notT) = 0.4$ e $m(T, notT) = 0.6$, indicativas de mau comportamento.

Assim, quanto maior a quantidade de testemunhas mentirosas, maior a probabilidade dos clientes nunca decidirem por interagir com os provedores bem comportados, tornando-se vítimas reincidentes deste ataque.

A figura 5.41 mostra que o método Bayesiano também sofre uma baixa significativa na reputação média dos seus provedores bem comportados.



(a) (b)

Figura 5.41: Exagero Negativo - Reputação Média dos Provedores Bem Comportados

A figura 5.42 mostra a influência exercida pelo ataque com o modelo de mentira complementar. Os métodos de média simples, dst e exponencial não demonstraram ser muito afetados por este ataque. Antes de descrever os motivos, alguns conceitos devem ser entendidos.

No início da simulação, quando os clientes são inexperientes, clientes honestos informam valores neutros (próximos de 0.5) a respeito dos provedores os quais ainda são incapazes de julgar. O interessante é que clientes mentirosos, que neste caso estão usando a fórmula 3.31 para calcular suas mentiras, também tendem a informar valores neutros quando não têm experiências. Isso quer dizer que, neste modelo, existe um período, que será chamado de período de honestidade acidental, no qual testemunhas mentirosas informam mentiras muito próximas dos verdadeiros valores que foram calculados.

Na mentira complementar, as testemunhas mentirosas aumentam sua capacidade de mentir à medida que vão ganhando experiências com os provedores e se tornando capazes de detectar quem são os bem e quem são os mal comportados. Esta característica aproxima mais este modelo de ataques reais que os demais, pois nos exageros positivo e negativo, quanto mais experiências um cliente tem com um provedor, menos ele consegue mentir sua reputação.

Numa rede P2P real, não parece fazer muito sentido, um *peer* que difama ou elogia fortemente outro sem nem mesmo conhecer seu comportamento. Ainda que fosse considerado um interesse gratuitos por parte dos mentirosos em prejudicar a rede, o ataque seria mais produtivo se estes *peers* detivessem o conhecimento dos provedores dos quais eles espalham as mentiras. Afinal, quando uma testemunha exagera negativamente um prove-

dor mal comportado ou quando exagera positivamente um provedor bem comportado, ela está, na realidade, ajudando os demais clientes a detectarem tais comportamentos.

O uso de exageros positivo e negativo ganha mais significado quando são considerados *peers* em conluio. Neste caso, os integrantes do grupo de conluio publicam elogios a respeito dos *peers* do grupo e difamam *peer* que estão fora, não importando seus comportamentos.

Retomando, agora, a análise dos comportamentos dos métodos de média simples, exponencial e dst, observa-se que estes três métodos têm uma característica em comum: os clientes iniciam a simulação associando peso 1 às informações de segunda mão e, à medida que vão preenchendo seus históricos (que nesta simulação é de tamanho 10), diminuem este peso até desprezarem totalmente as informações de segunda mão.

Este período, no qual estes métodos estão associando alto peso às informações de segunda mão, coincide com o período de honestidade acidental das testemunhas e, desta maneira, todos os clientes, mentirosos ou não, vão ganhando experiências simultaneamente ao longo da simulação. O que ocorre é que, quando as testemunhas mentirosas estão prontas para disseminar suas mentiras pela rede, se deparam com clientes que já ignoram ou associam valores muito baixos às informações de segunda mão. Nos demais métodos, onde os clientes usam as informações de segunda mão durante toda a simulação, os efeitos da mentira complementar são muito maiores.

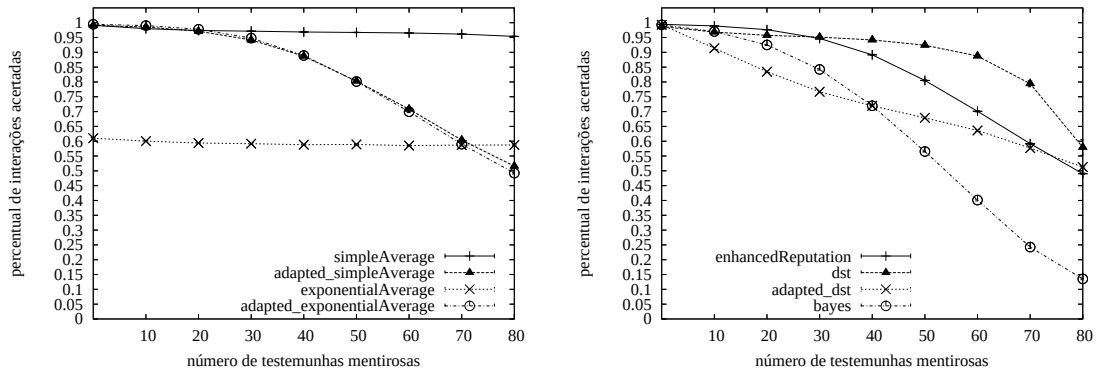
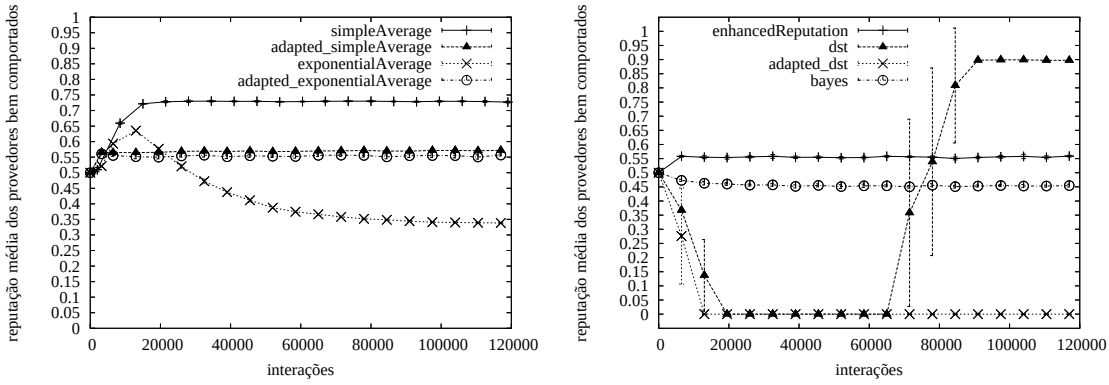


Figura 5.42: Mentira Complementar

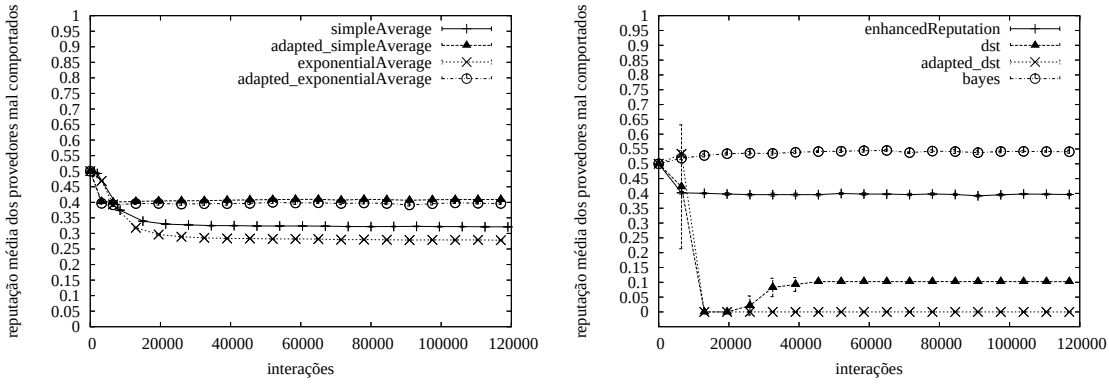
As figuras 5.43 e 5.44 mostram ainda como os valores de reputação média dos provedores bem e mal comportados foram afetados em cada método num ambiente que conside-

rou a presença de 60 clientes aplicando o ataque da mentira complementar. Estas figuras mostram um comportamento atípico dos métodos que usam a teoria de Dempster-Shafer.



(a) (b)

Figura 5.43: Mentira Complementar - Reputação Média dos Bons Provedores



(a) (b)

Figura 5.44: Mentira Complementar - Reputação Média dos Maus Provedores

Quando a regra de combinação de Dempter-Shafer é usada para combinar dois conjuntos de crenças que expressam absoluta certeza em hipóteses opostas, ou seja, $m(T) = 1$, $m(notT) = 0, m(T, notT) = 0$ e $m(T) = 0, m(notT) = 1, m(T, notT) = 0$, o resultado é $m(T) = 0/0$, $m(notT) = 0/0$, $m(T, notT) = 0/0$. Neste cenário, onde as testemunhas informam exatamente o contrário do que calcularam, é bastante provável acontecer esta situação na qual a combinação das informações de dois clientes bastante experientes sejam opostas, pois um deles é mentiroso.

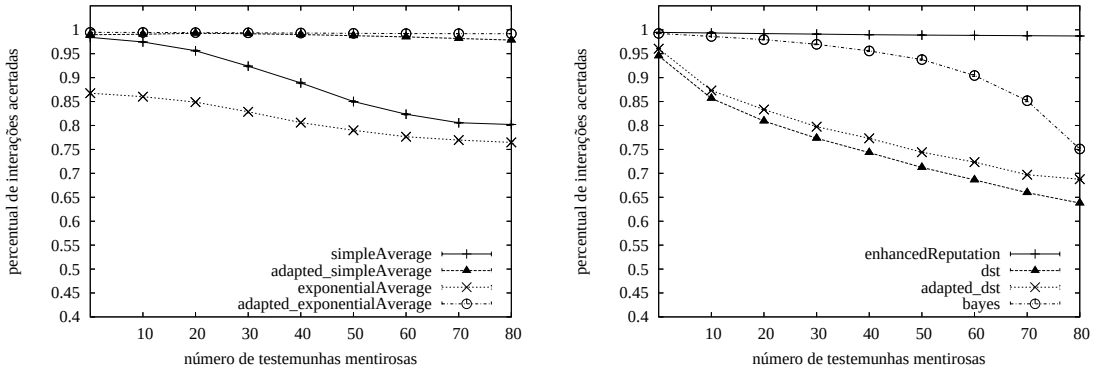
Os gráficos 5.43(b) e 5.44(b) mostram que, no início da simulação, até que os clientes adquiram experiências, ainda é possível combinar as crenças corretamente. Depois, am-

bos os métodos dst mostram valores de reputações médias nulas, causados pelo problema demonstrado no parágrafo anterior. O método dst, ao contrário do método dst adaptado, consegue recuperar seu desempenho. É que no método dst original, quando os clientes preenchem seus históricos, eles deixam de usar as informações de segunda mão e, conseqüentemente de usar a regra de combinação de Dempster-Shafer.

As simulações foram repetidas para históricos de tamanho 100. A figura 5.45 mostra os resultados obtidos quando o modelo de mentira usado é o exagero positivo. O modelo de média simples passa a ser mais afetado pelo aumento do número de testemunhas mentirosas. Com um histórico de tamanho grande, os clientes usam as informações de segunda mão por mais interações. Além disso, os clientes começam associando peso 1 às informações de segunda mão e desprezando as de primeira mão e, até que pelo menos metade dos históricos estejam preenchidos, as informações de segunda mão se mantêm com peso maior que as de primeira. Desta maneira, a exposição deste método aos ataques aumenta muito com o histórico de tamanho 100 e quanto mais testemunhas mentirosas existirem na rede, pior será seu desempenho.

A figura mostra que o modelo de média simples adaptado não sofreu os mesmos efeitos do modelo de média simples original, pois os clientes, em momento nenhum da simulação, deixaram de usar suas informações de primeira mão, associando desde o início um peso constante de valor 0.5 às informações de segunda mão.

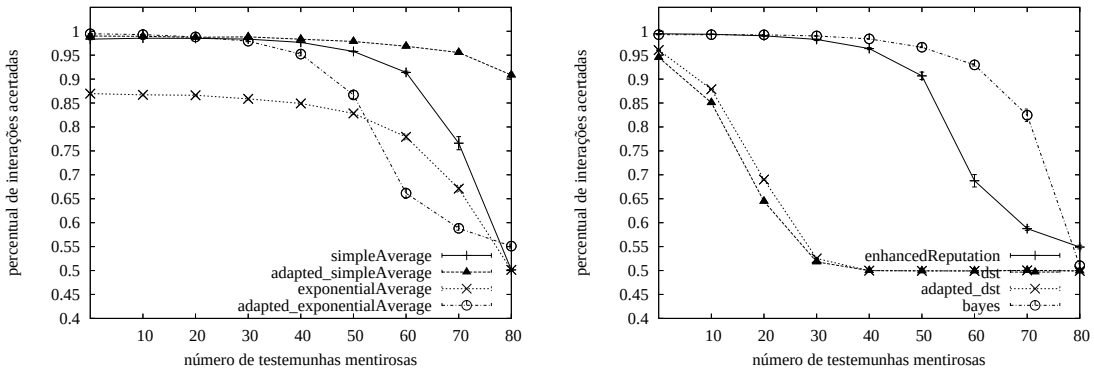
A figura 5.45 mostra ainda um aumento de desempenho para o método exponencial. Como já tinha sido visto anteriormente, este método realmente apresenta melhor comportamento quando é adotado um maior tamanho para os históricos. O método exponencial adaptado não foi afetado pelo tamanho de histórico. Quanto aos métodos que usam DST, seus desempenhos foram bem piorados, como já era esperado pelos resultados obtidos anteriormente para estes métodos quando o tamanho 100 de histórico foi considerado.



(a) (b)

Figura 5.45: Exagero Positivo - H = 100 - Percentual de Decisões Acertadas

A figura 5.46 mostra os resultados obtidos quando o tamanho de histórico adotado é 100 e o modelo de mentira usado é o exagero negativo. O comportamento do método de média simples e dos métodos que usam DST pioraram em comparação com os resultados obtidos das simulações do exagero negativo com históricos de tamanho 10. Já o método exponencial teve seu desempenho melhorado. Estes efeitos, idênticos aos observados na figura anterior, já eram esperados pelos motivos mencionados anteriormente. Eles se repetem também no modelo mentira complementar, conforme mostra a figura 5.47.



(a) (b)

Figura 5.46: Exagero Negativo - H = 100 - Percentual de Decisões Acertadas

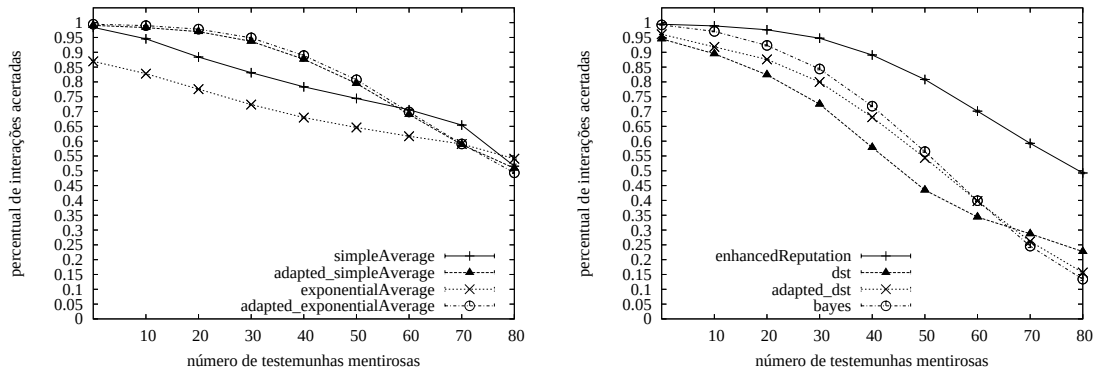
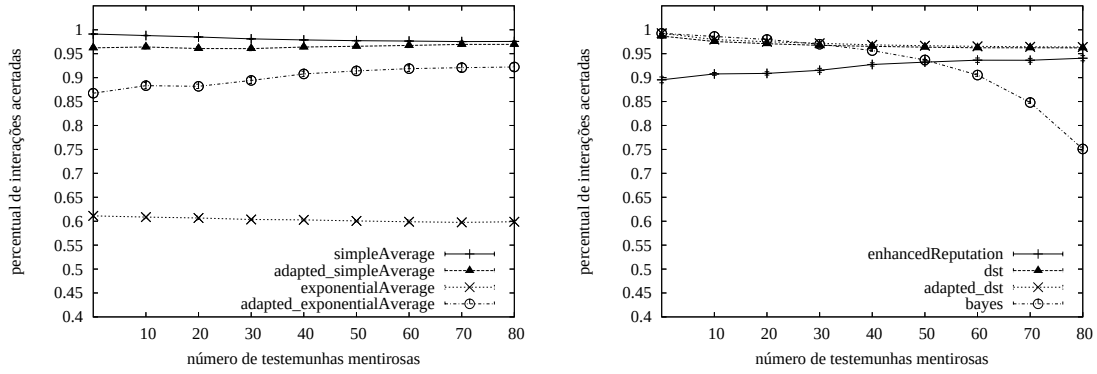


Figura 5.47: Mentira Complementar - H = 100 - Percentual de Decisões Acertadas

A figura 5.48 mostra os resultados obtidos quando o modelo de mentira configurado é o exagero positivo e o peso α, usado na equação 3.4 pelos métodos de média simples adaptado, exponencial adaptado e exponencial que não usa histórico, é configurado para 0.7. Foi considerado tamanho de histórico 10 nestas simulações.

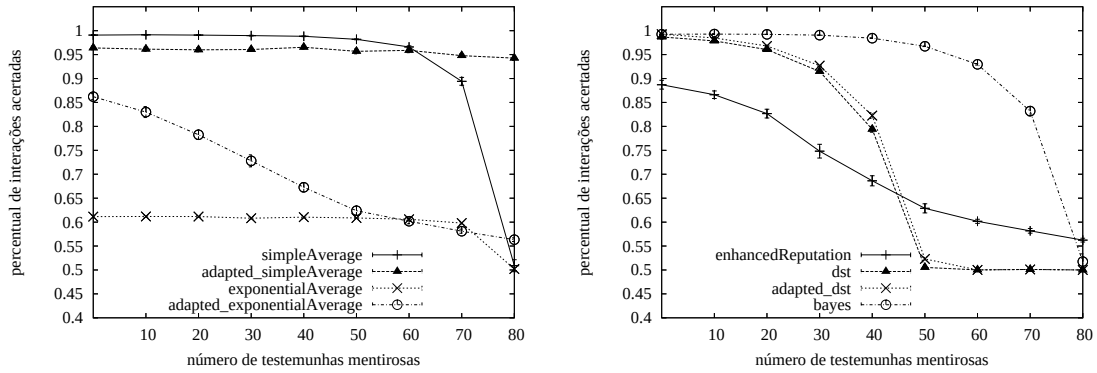
O método exponencial adaptado e o método exponencial sem histórico têm seus desempenhos piorados. Conforme já foi estudado, o maior peso dado às informações de primeira mão aumenta os erros de julgamento causados pela convergência exagerada promovida pelo uso do fator de decaimento. O método de média simples adaptado também sofre uma leve queda de desempenho em relação às simulações que consideraram o valor 0.5 para α. Embora este método não use fator de decaimento, o grande peso dado às informações de primeira mão desde o início da simulação pode causar alguns enganos nos casos em que provedores bem comportados falham em suas primeiras interações com clientes inexperientes.



(a) (b)

Figura 5.48: Exagero Positivo - α = 0.7 - Percentual de Decisões Acertadas

A figura 5.49 mostra efeitos similares quando o modelo adotado é o exagero negativo, ou seja, todos os métodos apresentaram pioras em seus desempenhos.



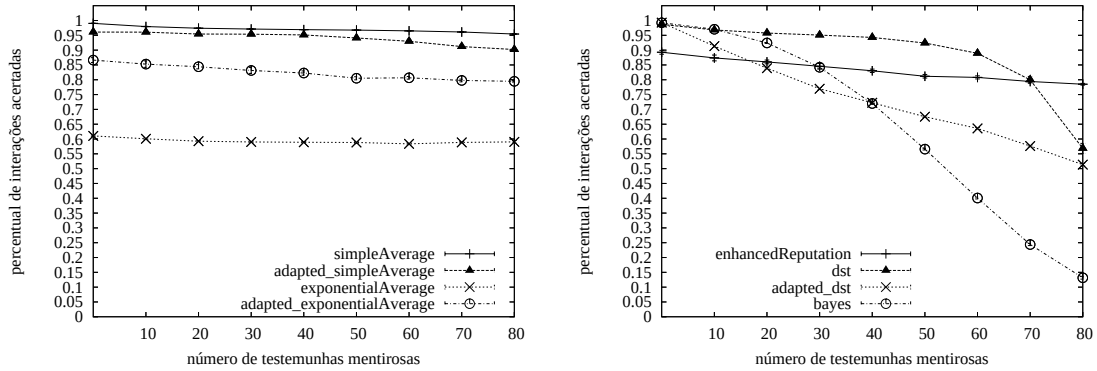
(a) (b)

Figura 5.49: Exagero Negativo - α = 0.7 - Percentual de Decisões Acertadas

A figura 5.50 mostra, que no caso do modelo de mentira complementar, o comportamento muda um pouco. A queda de desempenho em relação às simulações que consideraram $\alpha = 0.5$ só foi observada até que um certo número de testemunhas mentirosas. Pelo gráfico nota-se que, os métodos têm um aumento de desempenho nas simulações que consideram a presença de mais de 30 testemunhas mentirosas na rede.

As curvas do gráfico 5.50 mostram que num ambiente muito hostil, onde um grande percentual dos clientes mentem na hora de dar seu testemunho, um grande peso nas experiências próprias ajudam. Este é um raciocínio que faz bastante sentido, mas que impressionantemente, só foi válido para este modelo de mentira complementar.

Isso ocorre porque nos outros métodos, mesmo antes de terem oportunidade de acumular experiências com os provedores, os clientes eram vítimas de informações mentirosas. No modelo de mentira complementar, os clientes tiram proveito do período de honestidade acidental das testemunhas mentirosas para acumularem informações de primeira mão, das quais podem usufruir melhor com um maior peso α.



(a) (b)

Figura 5.50: Mentira Complementar - α = 0.7 - Percentual de Decisões Acertadas

Com relação ao método Bayesiano, foi notado, anteriormente, que este método apresenta bastante sensibilidade ao ataque do exagero positivo quando o número de testemunhas mentirosas cresce na rede. A figura 5.51 apresenta os resultados obtidos para o modelo de mentira exagero positivo quando foram usados valores de u diferentes de 1 (equações 3.16 e 3.17). Menores valores de u aumentam a convergência dos clientes e fazem com que as testemunhas mentirosas não tenham tanto sucesso em seus ataques.

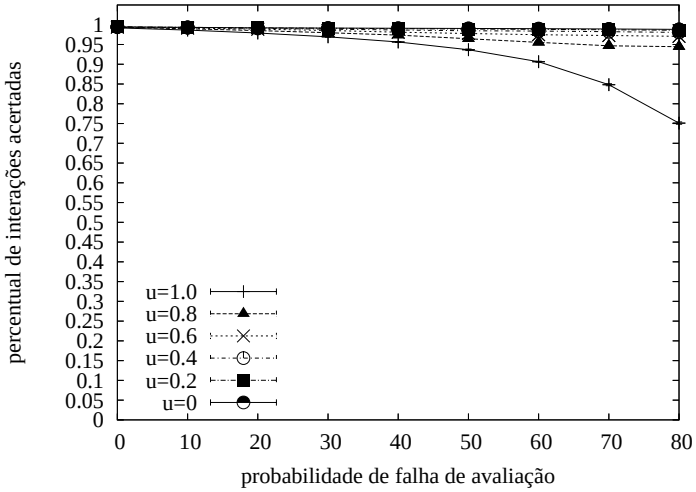


Figura 5.51: Exagero Positivo - Variação de u - Percentual de Decisões Acertadas

Com relação ao ataque que segue o modelo do exagero negativo, a figura 5.52 mostra que reduzir o valor de u até certo ponto não tem influência significativa no desempenho do método. Entretanto, quando este valor se torna muito baixo, o desempenho do método piora quando o número de testemunhas mentirosas na rede é alto. Isso porque, a convergência exagerada imposta pelo valor de u associada às informações de segunda mão provenientes de um grande número de clientes mentirosos que tentam fazer todos acreditarem que o comportamento dos provedores são piores do que realmente são, levam os clientes com muita facilidade ao mau julgamento.

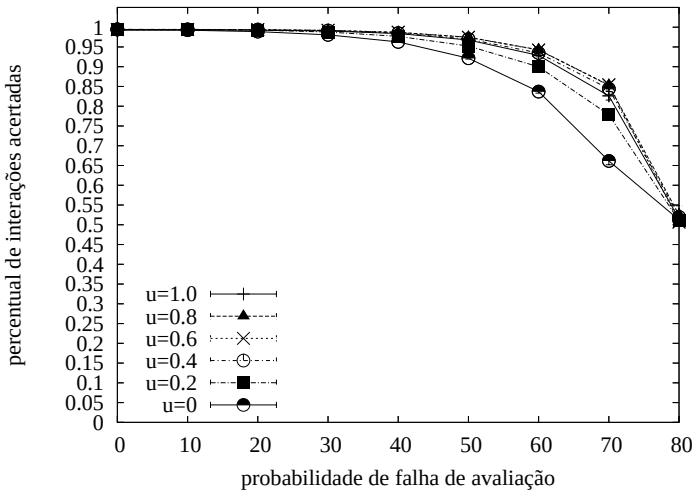


Figura 5.52: Exagero Negativo - Variação de u - Percentual de Decisões Acertadas

A figura 5.53 mostra o comportamento do método Bayesiano para a mentira complementar. A redução do valor de u praticamente não afeta o desempenho do método.

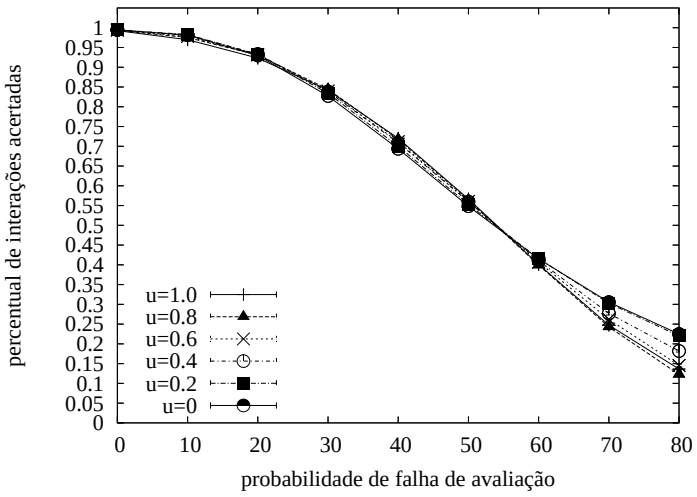
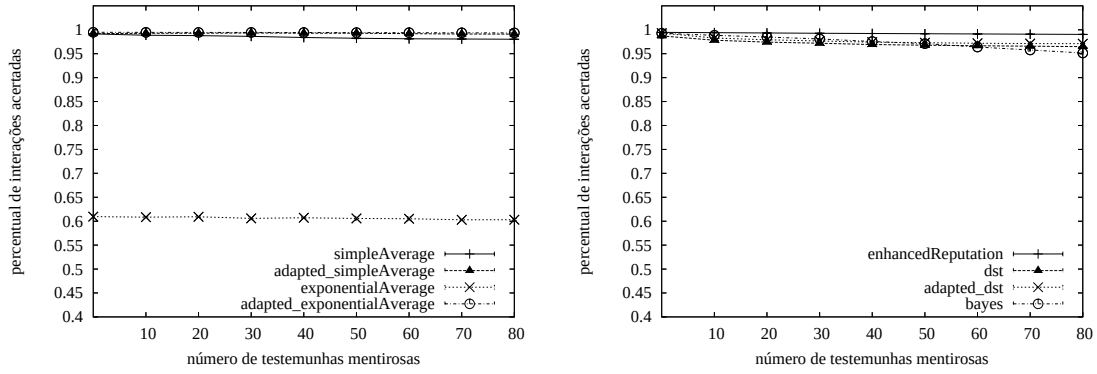


Figura 5.53: Mentira Complementar - Variação de u - Percentual de Decisões Acertadas

Até o presente momento, todas as simulações consideraram os modelos de exagero positivo e negativo usando $\sigma = 0.4$ em suas equações 3.29 e 3.30 respectivamente. Observando estas equações, espera-se que o aumento do valor de σ aumente a influência dos modelos de exagero nos métodos, causando neles uma maior queda de desempenho, enquanto que a redução de σ permitirá maiores percentuais de acerto.

Para demonstrar graficamente a influência deste parâmetro, as simulações que deram origem às curvas das figuras 5.38 e 5.40 foram repetidas considerando, valores diferentes para σ. Foram escolhidos os valores 0.3 e 0.5 para demonstrar os efeitos da redução e do aumento deste parâmetro nos desempenhos dos métodos.

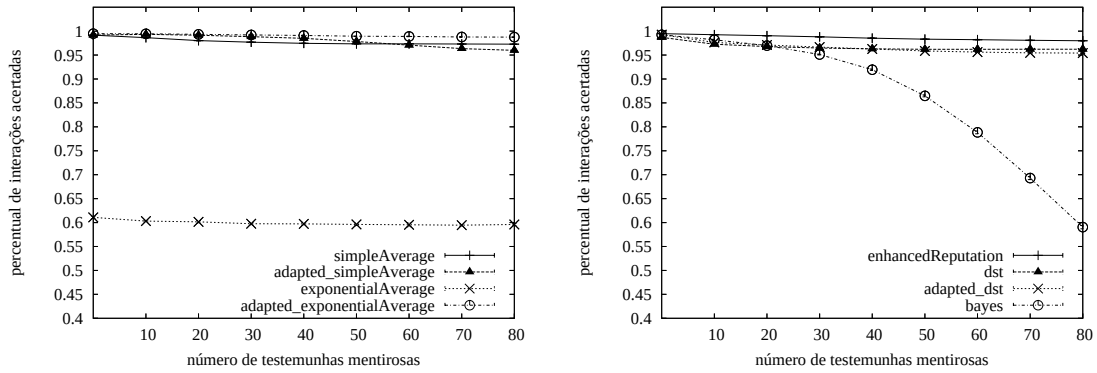
A figura 5.54 mostra que o menor valor associado a σ no modelo de exagero positivo diminuiu os efeitos deste ataque no método Bayesiano, que era o único a sofrer influência considerável do mesmo. Os demais, que já não eram muito prejudicado por este modelo de mentira, não sofreram alterações significativas.



(a) (b)

Figura 5.54: Exagero Positivo - σ = 0.3 - Percentual de Decisões Acertadas

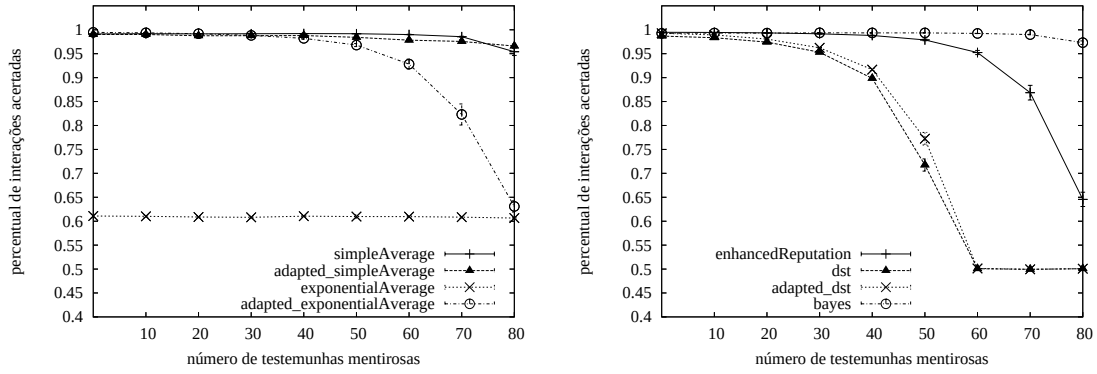
A figura 5.55 confirma que o aumento de σ causa uma queda no desempenho do método Bayesiano. Os demais métodos não sofreram grandes efeitos causados por esta mudança.



(a) (b)

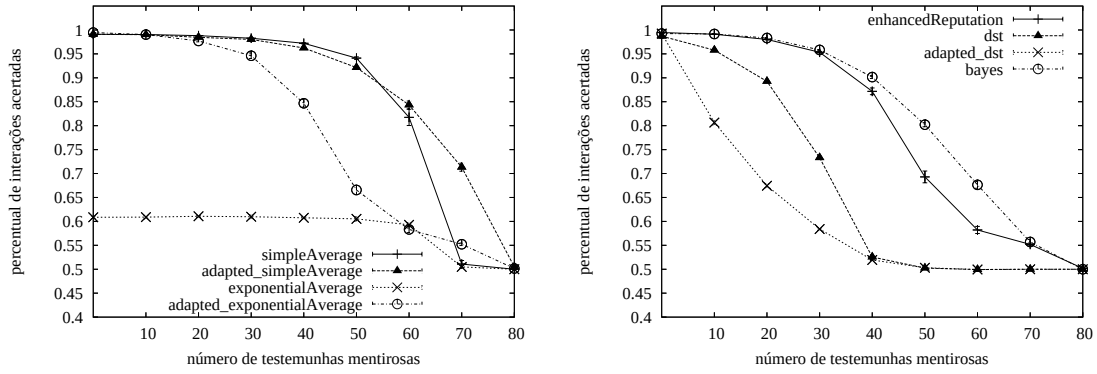
Figura 5.55: Exagero Positivo - σ = 0.5 - Percentual de Decisões Acertadas

A figura 5.56 mostra as novas curvas de percentuais de acertos dos métodos para o menor valor de σ adotado quando o modelo de mentira considerado é o exagero negativo. Como este modelo tem uma influência bem mais aparente em todos os métodos, é possível observar bem mais claramente como a redução do parâmetro σ diminui os efeitos negativos deste ataque nos métodos. Já a figura 5.57 demonstra exatamente o contrário, a perda de desempenho dos métodos de reputação em conseqüência do aumento de σ.



(a) (b)

Figura 5.56: Exagero Negativo - σ = 0.3 - Percentual de Decisões Acertadas



(a) (b)

Figura 5.57: Exagero negativo - σ = 0.5 - Percentual de Decisões Acertadas

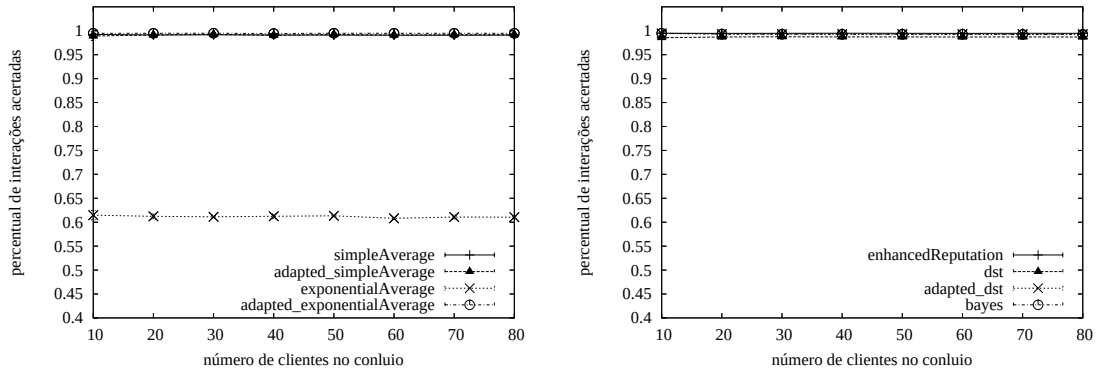
5.5 Cenário 5 - Testemunhas Mentirosas Agindo em Conluio

O Cenário 5 é bastante semelhante ao Cenário 4, entretanto, as testemunhas mentirosas da rede formam um grupo de conluio. O conjunto de simulações deste cenário mostra que agir em conluio é bastante interessante para clientes interessados em praticar o ataque do testemunho mentiroso, visto que assim estes clientes conseguem prejudicar os demais *peers* da rede sem serem prejudicados.

O primeiro conjunto de simulações considera então que as testemunhas mentirosas presentes na rede formam um grupo de conluio com os provedores mal comportados.

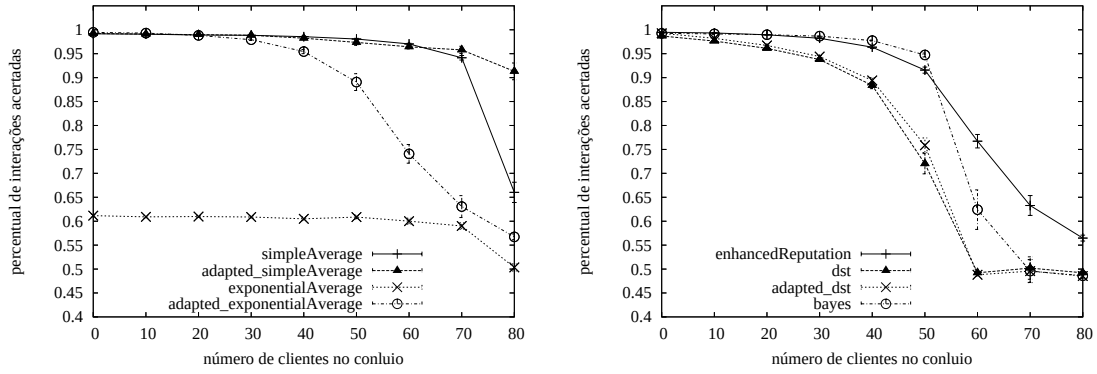
Como foi visto na seção 3.6.1 estes clientes mentirosos usam exagero positivo quando testemunham a respeito dos provedores do conluio para clientes que não participam do conluio. As testemunhas mentirosas seguem o modelo de exagero negativo quando testemunham a respeito dos provedores bem comportados, que não fazem parte do conluio, para clientes fora do grupo de conluio. Os *peers* mentirosos só não mentem quando trocam informações entre si. Foi considerado histórico de tamanho 10, fator de decaimento 0.6 e o peso α, usado pela equação 3.4, com valor 0.5.

A figura 5.58 mostra o percentual de decisões acertadas dos clientes que participam do conluio. Como é possível observar o desempenho de cada cliente é ditado apenas pelo desempenho do método de reputação adotado, tendo em vista que eles não se expõem às informações de segunda mão mentirosas. Tais clientes conseguem, através da formação do conluio prejudicar a rede sem sofrer nenhum dano em seus desempenhos. A figura 5.59 mostra a influência deste ataque no percentual de acertos dos *peers* que não estão participando do conluio.



(a) (b)

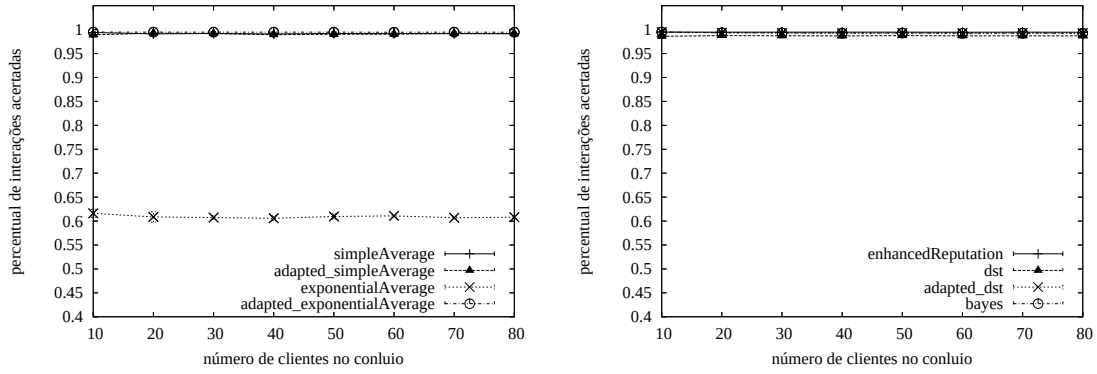
Figura 5.58: Percentual de Acertos dos Clientes do Conluio



(a) (b)

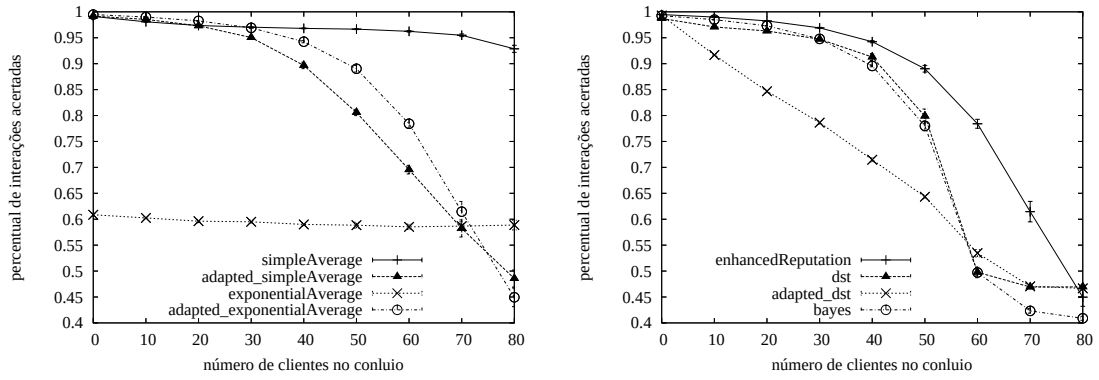
Figura 5.59: Percentual de Acertos dos Clientes Fora do Conluio

O segundo conjunto de simulações considera que as testemunhas mentirosas presentes na rede formam um grupo de conluio somente composto por clientes interessados em prejudicar a rede. Estes clientes usam mentira complementar quando testemunham para clientes que não participam do conluio e não mentem quando trocam informações entre si. Também foi considerado histórico de tamanho 10, fator de decaimento 0.6 e o peso α, usado pela equação 3.4, com valor 0.5.



(a) (b)

Figura 5.60: Conluio de Clientes - Percentual de Acertos dos Clientes do Conluio



(a) (b)

Figura 5.61: Conluio de Clientes - Percentual de Acertos dos Clientes Fora do Conluio

A figura 5.60 comprovou mais uma vez que o ataque em conluio oferece, aos *peers* que estão atacando a rede, a vantagem de não terem os desempenhos de seus métodos de reputação afetados. Já a figura 5.61 mostrou os prejuízos causados por este ataque aos clientes que estão fora do conluio.

5.6 Cenário 6 - O Uso da Credibilidade

Nesta seção, serão estudadas as influências exercidas pelos métodos de credibilidade descritos no capítulo 3.7. Conforme foi visto, os mecanismos de credibilidade têm o objetivo de tornar os *peers* da rede capazes de identificar testemunhas mentirosas para que, desta maneira, possam se expor menos às falsas informações que são oferecidas por elas.

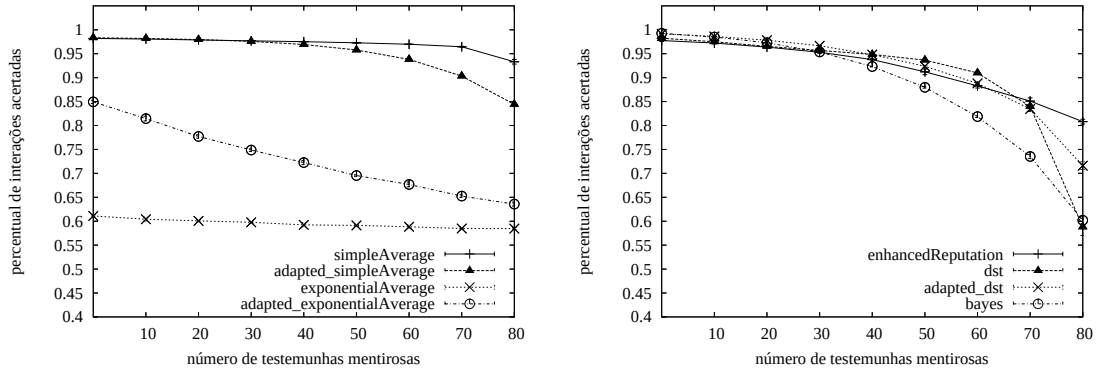
5.6.1 Método WMA

Para as simulações dos mecanismos de reputação trabalhando em conjunto com o mecanismo de credibilidade WMA (descrito na seção 3.7.1), foram configurados históricos de tamanho 10, fator de decaimento 0.6 e o peso, usado pela equação 3.4, igual a 0.5. Quanto às testemunhas mentirosas, foram configuradas para usar modelo de mentira complementar.

Conforme foi estudado na seção 3.7.1, a simulação deste mecanismo de credibilidade exige a configuração da constante β, que é usada pela equação 3.32. Se β for configurado com valor 1, os clientes sempre associarão credibilidade 1 às informações de segunda

mão que receberem. Sendo assim, os primeiros testes deste mecanismo consideram um valor ligeiramente mais baixo, o valor 0.9.

A figura 5.62 mostra os percentuais de acertos atingidos pelos clientes que utilizaram os métodos de reputação em conjunto com o WMA. Para análise das vantagens e desvantagens da utilização deste método de credibilidade, as curvas apresentadas por esta figura devem ser comparadas com as da figura 5.42, que mostram os percentuais de acertos dos métodos na presença de mentirosos utilizando a mentira complementar sem nenhum mecanismo de credibilidade em uso pelos clientes.



(a) (b)

Figura 5.62: WMA - β = 0.9 - Percentual de Decisões Acertadas

Seguindo este procedimento, a primeira observação notável é a severa perda de desempenho sofrida pelo método exponencial adaptado. Para explicar este fenômeno dois importantes aspectos precisam ser detalhados.

O primeiro deles é uma característica do mecanismo de credibilidade WMA: A testemunha nunca é premiada por falar a verdade. Quando a informação fornecida por uma testemunha é exatamente idêntica à experiência vivida pelo cliente que a requisitou, o valor calculado de θ (equação 3.32) é 1 e sua credibilidade, atualizada pela equação 3.33, mantém o valor anterior. Entretanto, por menor que seja a diferença entre a informação de segunda mão fornecida e a experiência vivida pelo cliente, a credibilidade será atualizada para um valor menor que o anterior.

Quanto menor o β escolhido para ser usado na equação 3.32, mais rapidamente cairão os valores de credibilidade calculados pelos clientes para suas testemunhas. Ao longo do tempo, estes valores de credibilidade se aproximarão de zero.

O segundo aspecto é que, para o caso do método exponencial adaptado, a equação 3.2 é usada para agregar as informações de segunda mão. Quanto menores os valores de credibilidade, menor será o valor do numerador da equação 3.2 e, em conseqüência, mais próximo de zero estará o valor das informações de segunda mão agregadas. Quando este valor muito reduzido é levado para a equação 3.4, que agrega primeira e segunda mão, a reputação tenderá para $\alpha * R(P_i, P_j)$.

O método exponencial adaptado sofre com o problema da convergência exagerada, já estudado em simulações anteriores, que faz com que poucas falhas cometidas por um provedor bem comportado sejam suficientes para reduzir muito o valor de reputação de primeira mão. Então, se o modelo de credibilidade WMA faz o cálculo final da reputação tender a $\alpha * R(P_i, P_j)$, os percentuais de acertos atingidos pelo método decairão.

A curva deste método mostra que só existe ganho com o uso em conjunto com o WMA quando o número de testemunhas mentirosas é muito grande, pois neste caso, embora os clientes encontrem dificuldades em identificar os provedores bem comportados, ao menos o uso somente de suas informações de primeira mão os tornam mais capazes de identificar os provedores mal comportados.

O método de média simples adaptado, embora também faça uso das equações 3.2 e 3.4 em seus cálculos de reputação, não tem a mesma velocidade de convergência do método exponencial adaptado e, neste valor de β escolhido, consegue até melhorar seu desempenho. Ainda assim, como será visto posteriormente, menores valores de β, que farão as credibilidades calculadas reduzirem mais rapidamente, afetarão seu desempenho.

Além dos métodos de média simples adaptado e de média exponencial adaptado, outro método que usa a equação 3.4 no cálculo final da reputação é o método exponencial sem histórico. Entretanto, seu comportamento é bem diferente dos demais, pois o intervalo de valores considerado para a reputação é $[-1, 1]$.

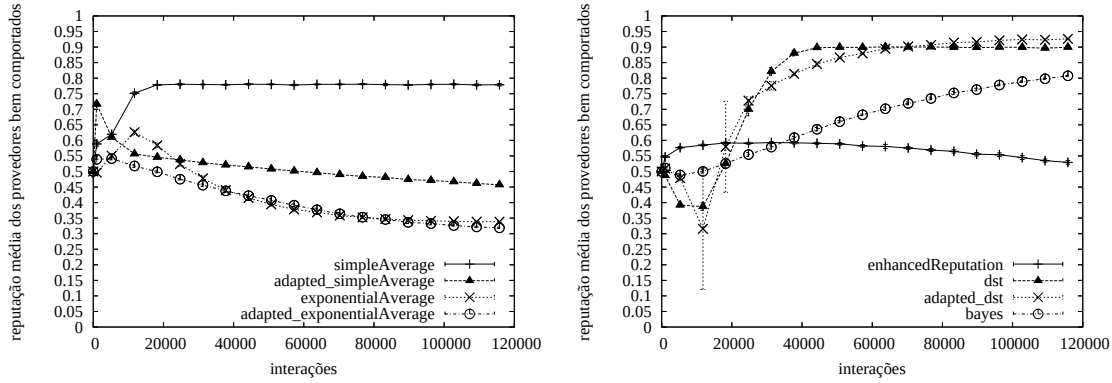
O resultado da agregação das informações de segunda mão, que é feita pela equação 3.8, também tende a zero quando o cliente associa às testemunhas valores muito baixos de credibilidade. Porém, enquanto que no intervalo $[0, 1]$, zero significa um péssimo comportamento para o provedor, no intervalo $[-1, 1]$, é um valor neutro. Desta forma, no cálculo do valor final de reputação, quando um cliente que não confia nas testemunhas que consultou usa a equação 3.4, o valor de primeira mão está sendo combinado com um valor neutro, e não com um valor muito baixo, que colaboraria para o aumento da

incidência de maus julgamentos dos provedores bem comportados.

O único problema é que este método, como qualquer método exponencial, tem uma rápida convergência, então, se menores valores são adotados para β, a credibilidade atinge valores próximos de zero mais rapidamente, o método passa a depender somente de suas informações de primeira mão e apresenta uma leve queda de desempenho em virtude dos maus julgamentos. Ainda assim, seu desempenho é bem melhor que os demais métodos exponenciais que trabalham no intervalo $[0, 1]$.

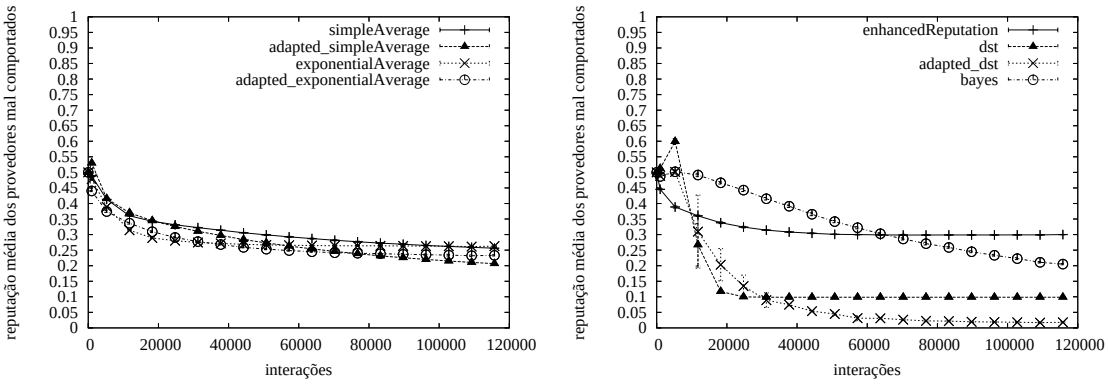
Os métodos de média simples, média exponencial e de Dempster-Shafer originais são pouco afetados pelo uso do método WMA tendo em vista que eles usam as informações de segunda mão agregadas por um curto período de tempo, somente enquanto os clientes não preencheram seus históricos. Já os métodos de Dempster-Shafer adaptado e Bayesiano ganham bastante em desempenho já que desprezar os valores de segunda mão os deixa livres da forte influência que lhe causavam as testemunhas mentirosas.

As figuras 5.63 e 5.64 mostram ainda como os valores de reputação média dos provedores bem e mal comportados foram afetados em cada método num ambiente que considerou a presença de 60 clientes aplicando o ataque da mentira complementar e clientes usando WMA. Para melhor entendimento das influências sofridas pelos métodos de reputação, estas figuras devem ser comparadas com as figuras 5.43 e 5.44.



(a) (b)

Figura 5.63: WMA - β = 0.9 - Reputação Média dos Provedores Bem Comportados



(a) (b)

Figura 5.64: WMA - β = 0.9 - Reputação Média dos Provedores Mal Comportados

A figura 5.63(a) mostra que o uso do WMA praticamente não alterou o comportamento dos métodos de média simples e exponencial. Como foi dito, anteriormente, estes métodos deixam de usar as informações de segunda mão quando seus históricos estão preenchidos e, portanto, a adoção de mecanismos de credibilidade não faz muita diferença. Esta figura mostra ainda a queda nos valores de reputação média calculados pelo método exponencial adaptado para os provedores bem comportados até valores abaixo do patamar indicativo de mal comportamento.

Uma queda bem mais sutil também é observada para o método de média simples adaptado. Neste caso, entretanto, a reputação média decai apenas até valores neutros, o que não faz com que os clientes deixem de interagir com estes provedores. Por este motivo, este método conseguiu maiores percentuais de acertos.

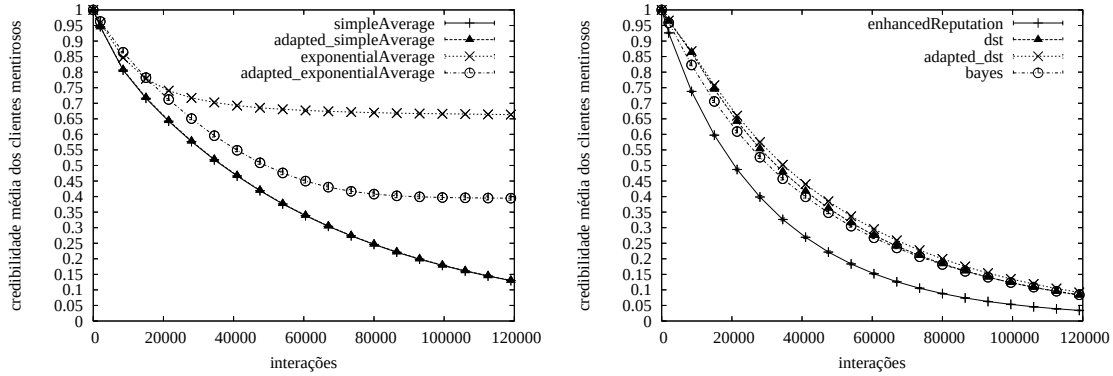
A figura 5.63(b) mostra que a reputação média calculada para o método exponencial sem histórico não sofre grandes alterações. Já os métodos que usam DST e o Bayesiano conseguem melhorar os valores de reputação calculados para os provedores bem comportados, atingindo índices acima de valores neutros, dentro do intervalo de valores indicativo de bom comportamento. O uso do WMA conseguiu, inclusive, impedir os efeitos, causados nos métodos dst original e adaptado, da combinação de crenças que expressam completa certeza em hipóteses completamente opostas, conforme visto na seção 5.4.

A figura 5.64 mostra que o uso do WMA proporcionou cálculo de valores de reputação média mais baixos para os provedores mal comportados na maior parte dos métodos, demonstrando grande melhora nos valores calculados pelo método Bayesiano.

As figuras 5.65 e 5.66 mostram as curvas de evolução da credibilidade média dos

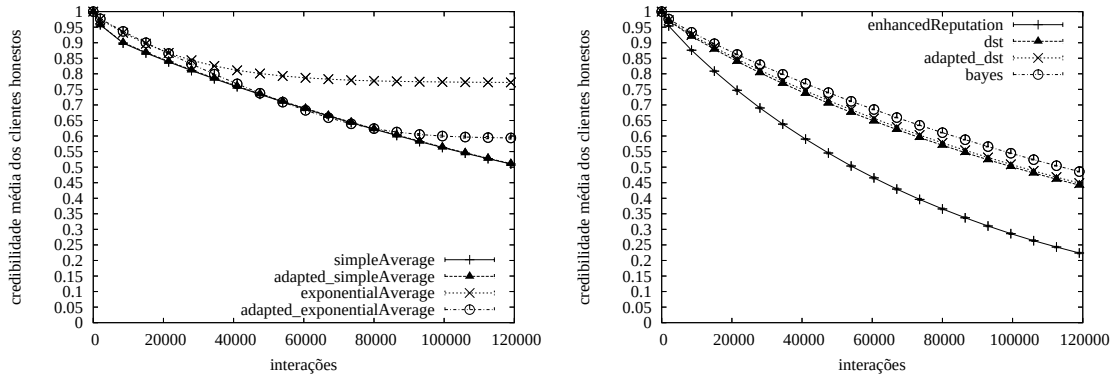
clientes mentirosos e honestos, respectivamente, ao longo da simulação calculada pelo WMA trabalhando em conjunto com cada método de reputação quanto existem 20 testemunhas mentirosas na rede. Observa-se que, como havia sido explicado, o valor de credibilidade tende a decrescer tanto para os clientes honestos quanto para os mentirosos. As únicas exceções são os métodos exponencial e exponencial adaptado.

Como ambos os métodos se tornam vítimas de sua própria convergência exagerada e param de interagir com os provedores bem comportados, além de parar de interagir com os ruins, seus valores de credibilidade estabilizam. Afinal, sem fazer interações, os clientes não tem como checar as informações de segunda mão recebidas e atualizar os valores de credibilidades.



(a) (b)

Figura 5.65: WMA - Credibilidade Média das Testemunhas Mentirosas

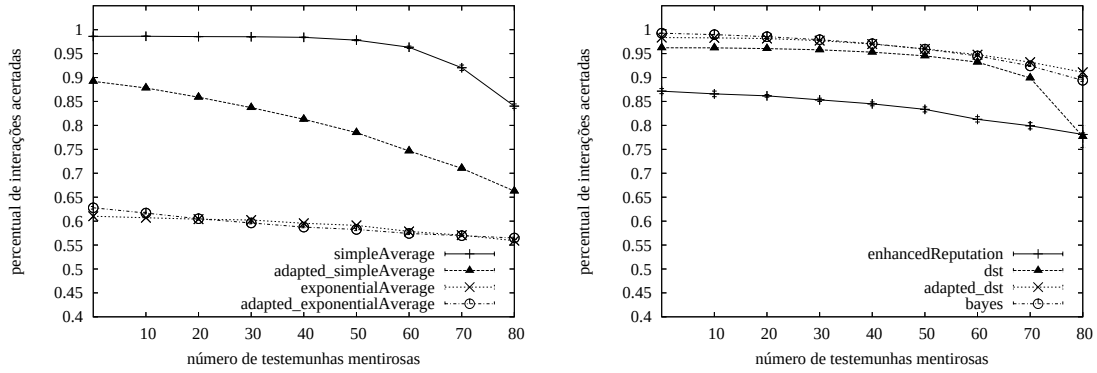


(a) (b)

Figura 5.66: WMA - Credibilidade Média das Testemunhas Honestas

A figura 5.67 mostra os percentuais de acertos atingidos pelos métodos quando a

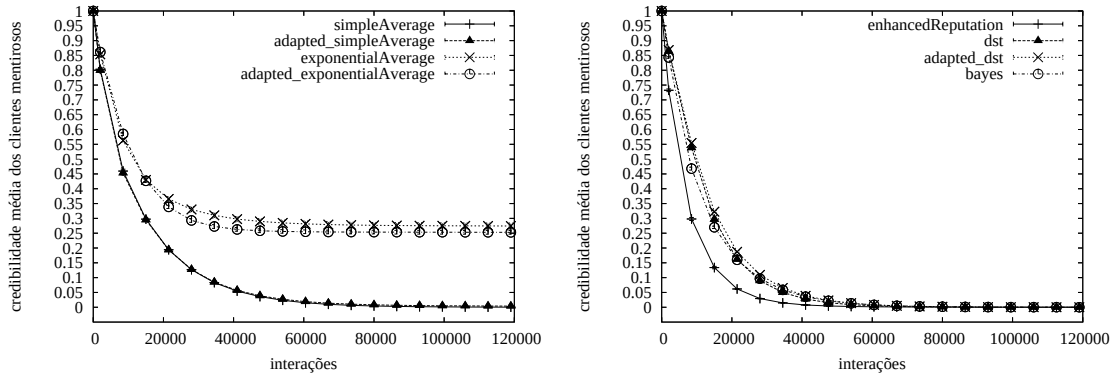
simulação é repetida considerando o valor 0.6 para a constante β (equação 3.32). Como esperado, houve queda de desempenho nos métodos que usam as equações 3.3 ou 3.4 no cálculo final de reputação. Os demais métodos, ou seja, dst, dst adaptado e bayes melhoraram seus desempenhos nas simulações com muitas testemunhas mentirosas.



(a) (b)

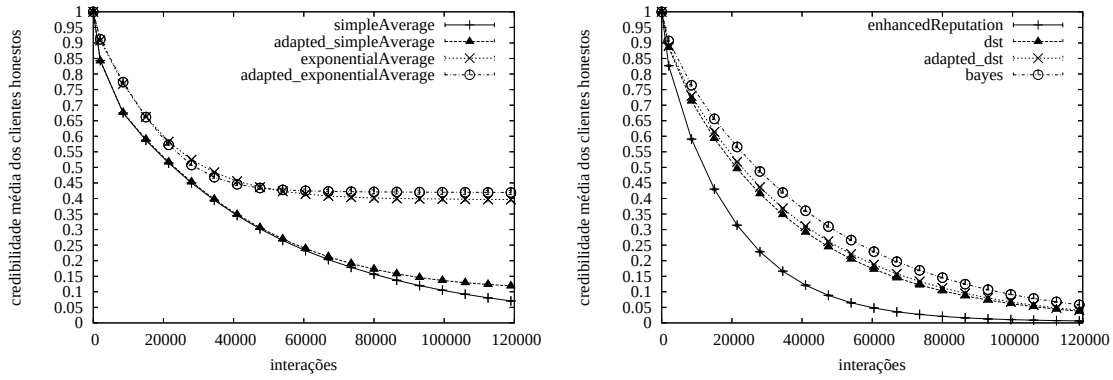
Figura 5.67: WMA - β = 0.6 - Percentual de Decisões Acertadas

As figuras 5.68 e 5.69 mostram as curvas de evolução da credibilidade média dos clientes mentirosos e honestos, respectivamente, ao longo da simulação calculada pelo WMA trabalhando em conjunto com cada método de reputação quanto existem 20 testemunhas mentirosas na rede e $\beta = 0.6$. Observa-se que, as curvas de credibilidade tendem a decrescer mais rapidamente, conforme havia sido explicado anteriormente.



(a) (b)

Figura 5.68: WMA - Credibilidade Média das Testemunhas Mentirosas



(a) (b)

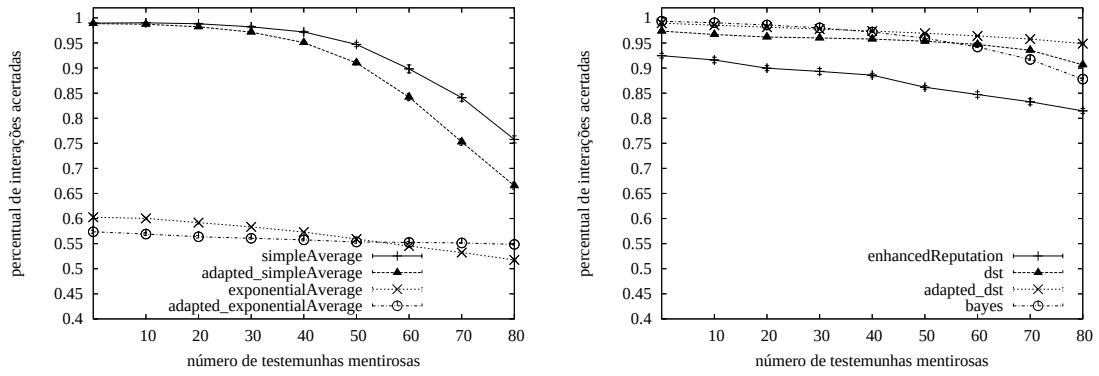
Figura 5.69: WMA - Credibilidade Média das Testemunhas Honestas

5.6.2 Método Bayesiano de Credibilidade

O método Bayesiano de Credibilidade foi descrito na seção 3.7.2. Tal como foi feito para o método WMA, as simulações deste mecanismo consideraram testemunhas mentirosas usando modelo de mentira complementar. Quanto à configuração dos métodos de reputação, foi considerado tamanho de histórico 10, fator de decaimento 0.6 e o peso, usado pela equação 3.4, igual a 0.5.

Conforme descrito na seção 3.7.2, a simulação deste método exige a configuração de dois parâmetros: o limiar de desvio d, usado durante o teste de desvio que é feito pela equação 3.20, e o fator ρ, usado pelas equações 3.35 e 3.36.

A figura 5.70 mostra os percentuais de acertos atingidos pelos clientes que utilizaram os métodos de reputação em conjunto com este mecanismo de credibilidade quando os valores adotados para d e ρ foram 0.1 e 1 respectivamente. Para análise das vantagens e desvantagens da utilização deste método, as curvas apresentadas por esta figura devem ser comparadas com as da figura 5.42, que mostram os percentuais de acertos dos métodos na presença de mentirosos utilizando a mentira complementar sem nenhum mecanismo de credibilidade em uso pelos clientes.



(a) (b)

Figura 5.70: Método Bayesiano - d = 0.1 e ρ = 1 - Percentual Médio de Acertos

Quando um valor muito baixo é escolhido para d, o teste de desvio torna-se muito rigoroso, pois passa a exigir que o testemunho recebido seja praticamente igual à experiência vivida pelo cliente. A figura 5.70 mostra que o método de média simples perde um pouco de desempenho quando o número de testemunhas mentirosas na rede é alto. Neste caso, o rigor do teste de desvio faz com que a credibilidade das testemunhas mentirosas caiam antes mesmo que os clientes tenham a chance de preencherem seus históricos.

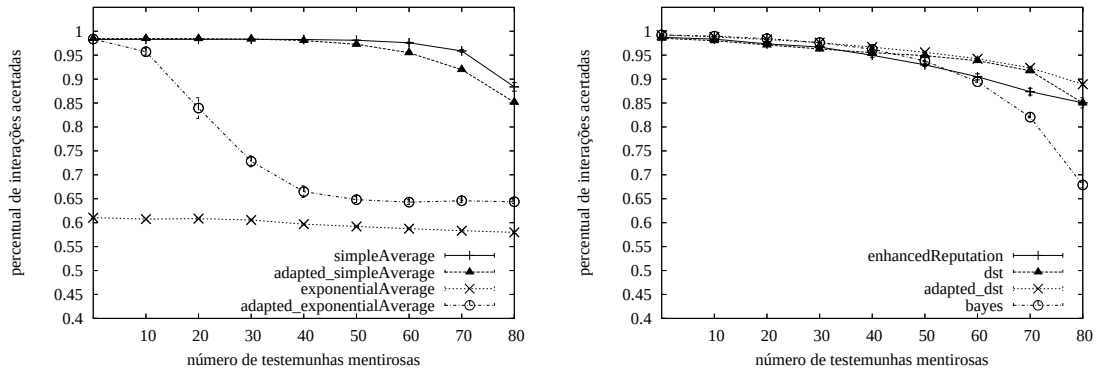
Desta maneira, quando o método for combinar seu valor de reputação de primeira mão com o de segunda mão, se a maior parte das testemunhas consultadas forem mentirosas e seus valores de credibilidade já estiverem próximos de zero, o valor final de reputação, calculado pela equação 3.3, tenderá a $\eta * R(P_i, P_j)$, ou seja, resultará em um valor bem mais baixo que a reputação de primeira mão. Esse fenômeno leva, em algumas ocasiões, ao mau julgamento de provedores bem comportados, o que reduz o percentual de acertos do método.

Raciocínio semelhante pode ser aplicado ao método de média simples adaptado, que associa às informações de segunda mão peso constante ao longo de toda a simulação (equação 3.4) e tem seu valor final de reputação reduzido a $\alpha * R(P_i, P_j)$. No caso dos métodos exponenciais, a rápida convergência do cálculo da reputação de primeira mão aliada a este efeito causado pela queda dos valores de credibilidade, faz com que estes métodos sofram bastante com o mau julgamento dos provedores bem comportados neste valor de d, apresentando maiores quedas de desempenho do que as demonstradas na figura 5.62 pelo mecanismo WMA.

Com relação aos demais métodos, dst, dst adaptado e bayes, que não utilizam as

equações 3.3 e 3.4 no cálculo final da reputação, apresentaram bons desempenhos em virtude da queda das credibilidades, que faz com que os clientes deixem de usar as informações de segunda mão, não se tornando vítimas das testemunhas mentirosas.

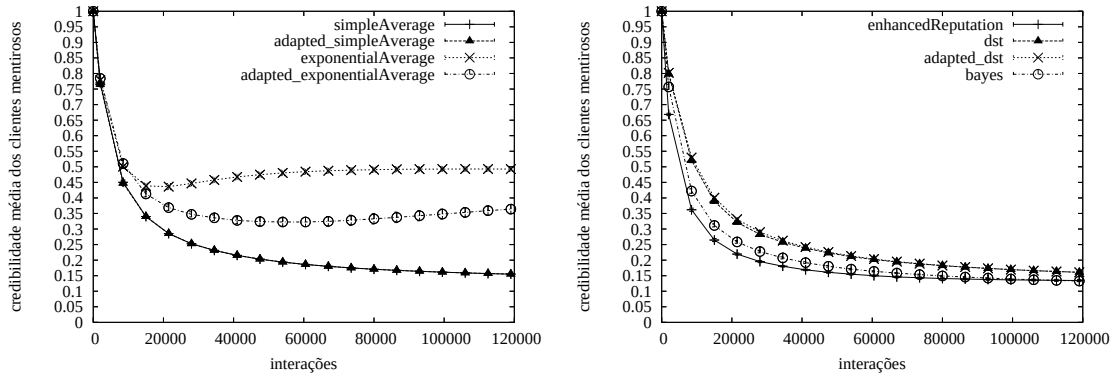
Com o teste de desvio um pouco mais tolerante, conforme mostra a figura 5.71, os métodos que usam a equação 3.3 ou a 3.4 aumentaram seu desempenho. Os demais não apresentaram grandes diferenças em seus percentuais de acertos.



(a) (b)

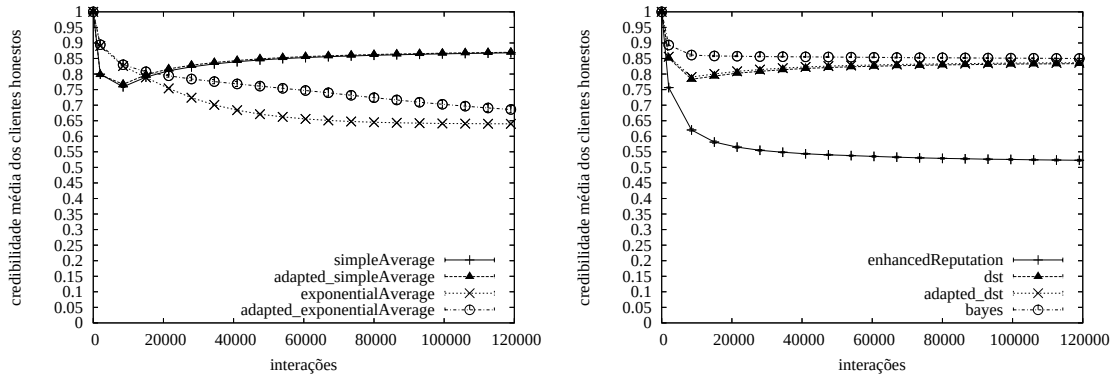
Figura 5.71: Método Bayesiano - d = 0.3 e ρ = 1 - Percentual Médio de Acertos

As figuras 5.72 e 5.73 mostram as curvas de evolução da credibilidade média dos clientes mentirosos e honestos, respectivamente, ao longo da simulação quanto existem 20 testemunhas mentirosas na rede e $d = 0.3$.



(a) (b)

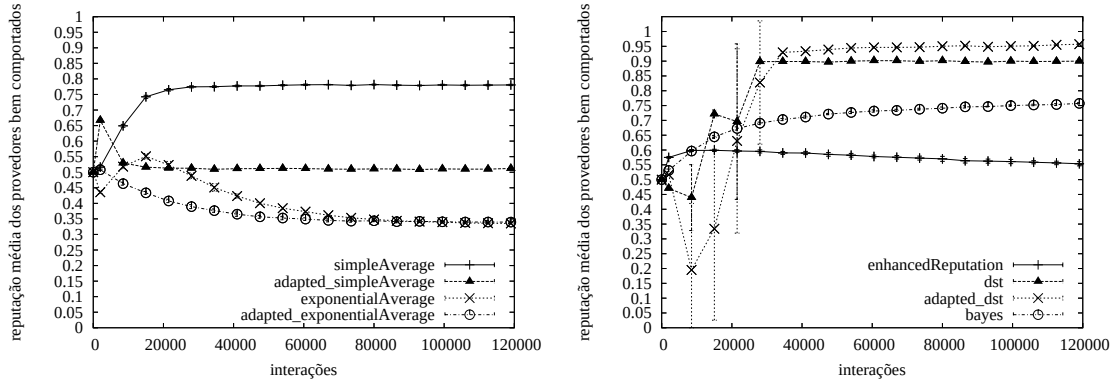
Figura 5.72: Método Bayesiano - Credibilidade Média das Testemunhas Mentirosas



(a) (b)

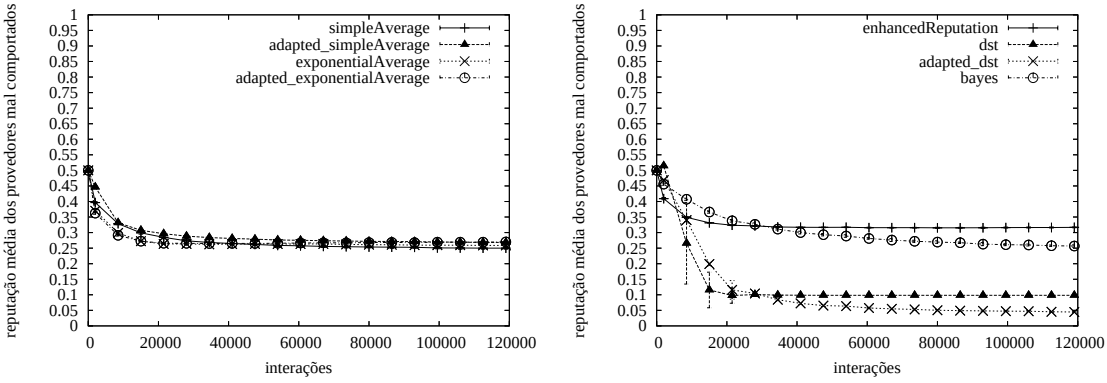
Figura 5.73: Método Bayesiano - Credibilidade Média das Testemunhas Honestas

As figuras 5.74 e 5.75 mostram ainda como os valores de reputação média dos provedores bem e mal comportados foram afetados em cada método num ambiente que considerou a presença de 60 clientes aplicando o ataque da mentira complementar. Observa-se pelos gráficos de reputação média que o cálculo das reputações provedores bem e mal comportados se tornaram mais eficientes principalmente nos métodos dst, dst adaptado e Bayesiano, se comparados às curvas das figuras 5.63 e 5.64 conseguidas pelo WMA.



(a) (b)

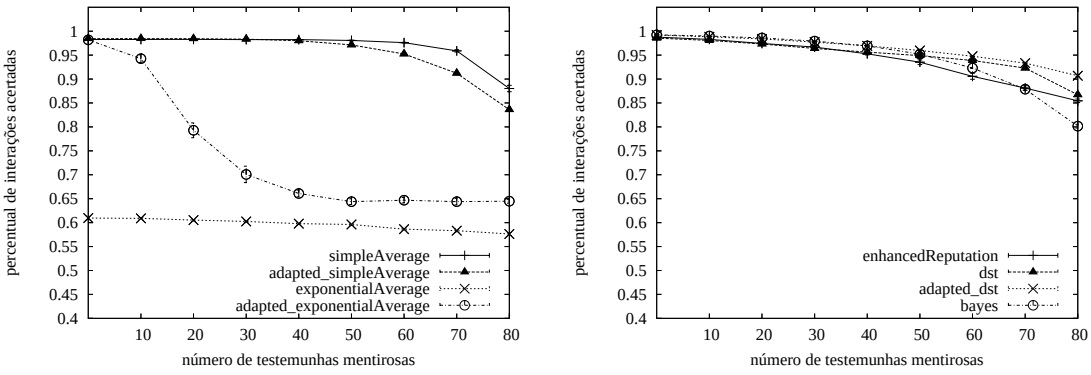
Figura 5.74: Método Bayesiano - d = 0.3 - Reputação Média dos Bons Provedores



(a) (b)

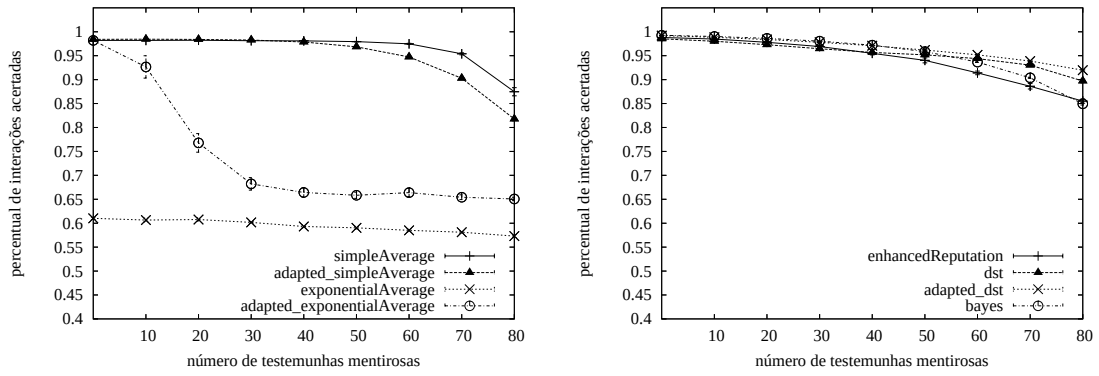
Figura 5.75: Método Bayesiano - d = 0.3 - Reputação Média dos Maus Provedores

A adoção de valores mais reduzidos de ρ não proporciona diferenças significativas de desempenho nos métodos, conforme mostram as figuras 5.76 e 5.77.



(a) (b)

Figura 5.76: Método Bayesiano - d = 0.3 e ρ = 0.9 - Percentual Médio de Acertos



(a) (b)

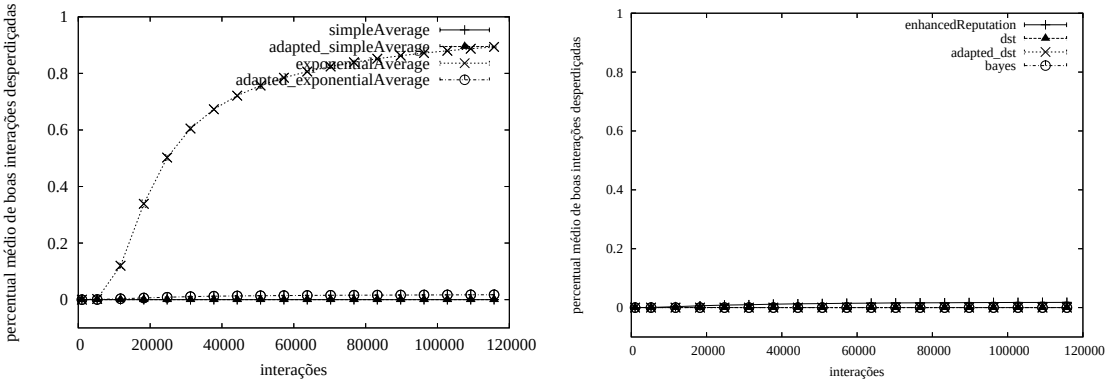
Figura 5.77: Método Bayesiano - d = 0.3 e ρ = 0.6 - Percentual Médio de Acertos

5.7 Cenário 7 - Clientes Escolhendo seus Provedores

Para o Cenário 7, o simulador foi configurado em modo de lista gerenciável de provedores, onde cada cliente é capaz de gerenciar sua própria lista de provedores ordenada por reputação, a partir da qual escolhe o provedor com quem deseja interagir.

Nas primeiras simulações, foi considerado que metade dos provedores são mal comportados, as testemunhas são escolhidas aleatoriamente durante a geração de cenário e não há clientes aplicando o ataque do testemunho mentiroso. Além disso, os métodos que usam históricos de avaliações foram configurados para usarem tamanho de históricos 10; os métodos que usam a equação 3.4 foram configurados para trabalharem com o peso α igual a 0.5 e o fator de decaimento escolhido, usado pelos métodos exponenciais, foi 0.6.

A figura 5.78 mostra o percentual médio de interações que foram desperdiçadas, ou seja, interações nas quais os clientes não conseguiram detectar nenhum provedor bem comportado e decidiram desistir da interação. Como pode ser observado, somente o método exponencial apresentou um percentual significativo de perdas, resultado já esperado, pois sua convergência exagerada fez com que os clientes julgassem de maneira errada os provedores bem comportados ao longo da simulação.

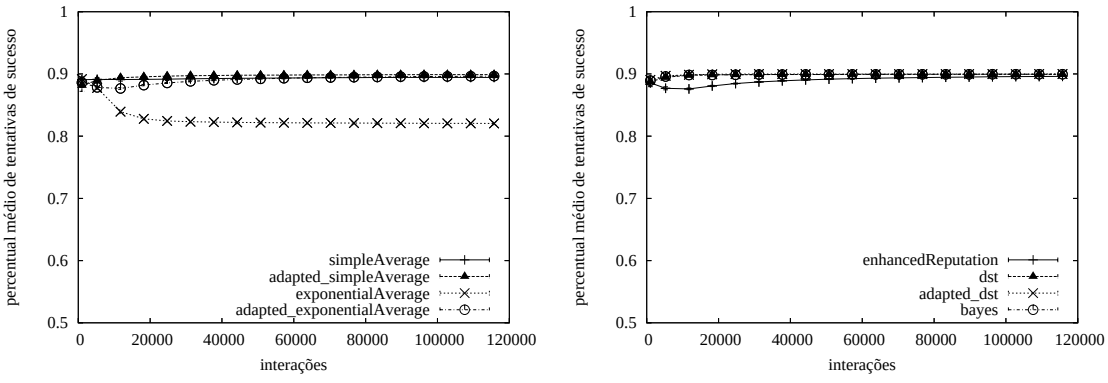


(a) (b)

Figura 5.78: Percentual Médio de Interações Perdidas

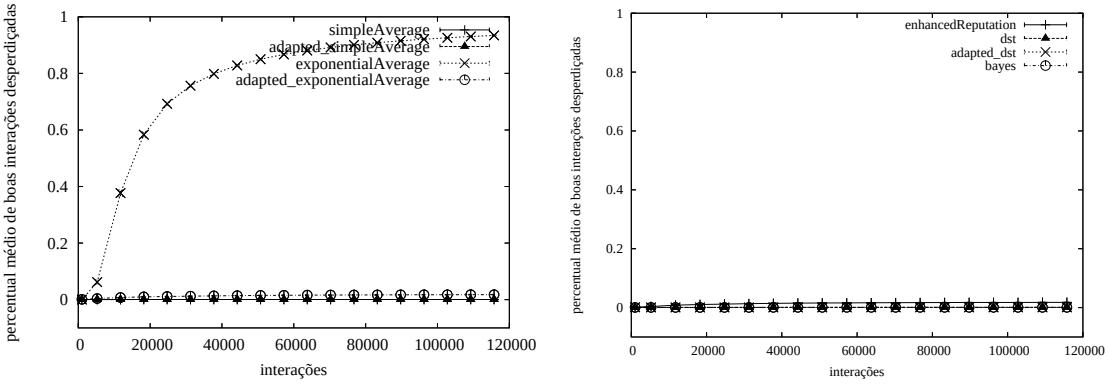
A figura 5.79 mostra o percentual médio de sucessos nas tentativas executadas pelos clientes. A maior parte dos métodos atingiu um alto percentual demonstrando que, ao longo da simulação, os clientes não precisaram fazer muitas tentativas para acertarem em suas escolhas e requisitarem seus pedidos a provedores bem comportados. O percentual mais baixo foi atingido pelo método exponencial e esse percentual só não foi menor porque os clientes, depois de terem julgado mal todos os provedores bem comportados, deixaram de fazer tentativas e passaram a desistir de todas as interações por acharem que não existia mais provedores a quem enviar requisições.

As figuras 5.80 e 5.81 mostram que resultados semelhantes foram encontrados para o cenário que considerou um percentual maior de provedores mal comportados na rede. Neste cenário, 70% dos provedores presentes na rede são mal comportados.



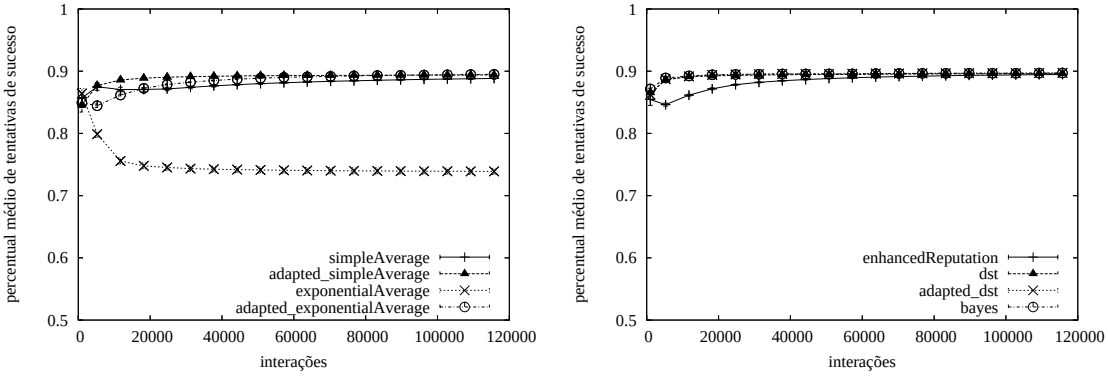
(a) (b)

Figura 5.79: Percentual Médio de Tentativas de Sucesso



(a) (b)

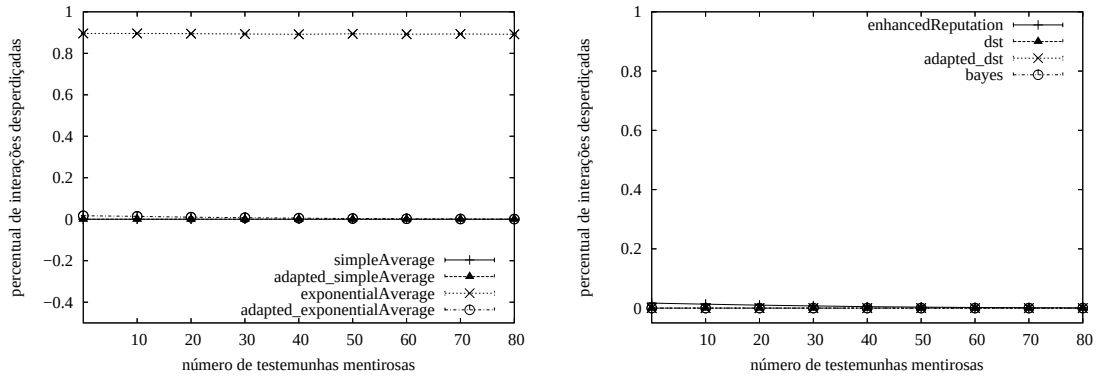
Figura 5.80: 70% Mal Comportados - Percentual Médio de Interações Perdidas



(a) (b)

Figura 5.81: 70% Mal Comportados - Percentual Médio de Tentativas de Sucesso

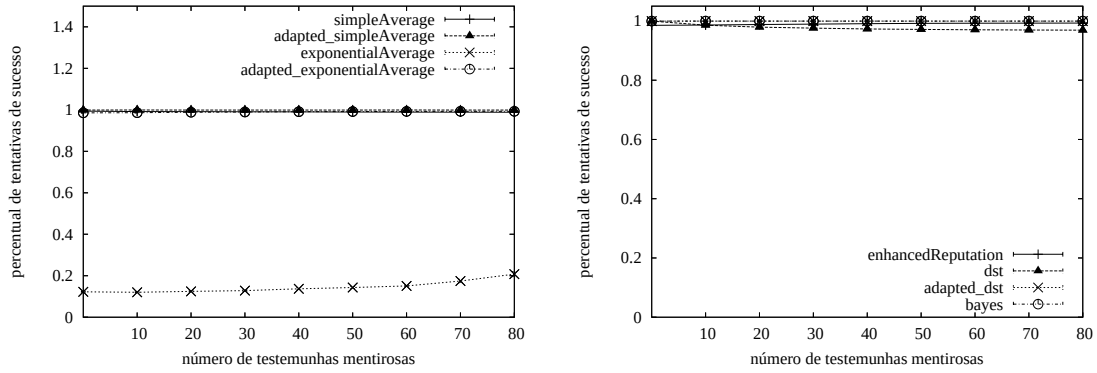
A figura 5.82 mostra as curvas de perda conseguidas a partir das simulações de cenários que consideraram a presença de testemunhas mentirosas aplicando o exagero positivo. Como pode ser observado, este ataque não teve influência significativa no percentual de interações desperdiçadas, nem mesmo quando o número de testemunhas mentirosas aumentou muito na rede.



(a) (b)

Figura 5.82: Exagero Positivo - Percentual de Interações Perdidas

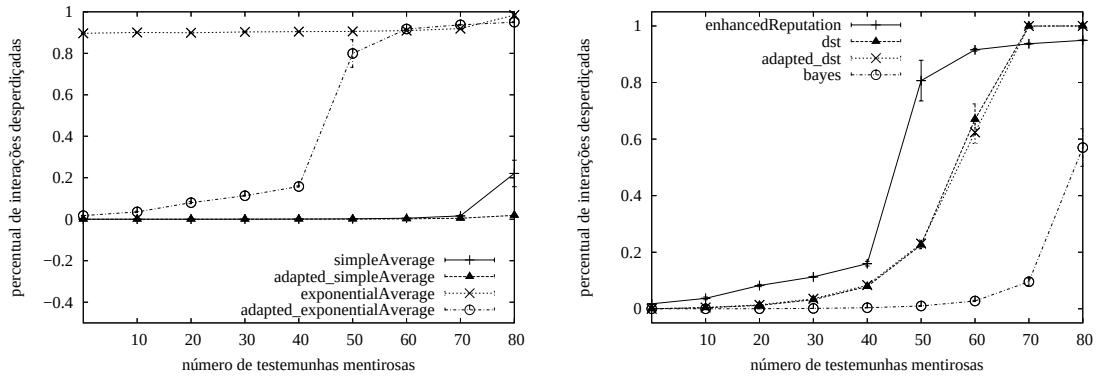
Já a figura 5.83 mostra que apenas o percentual das tentativas de sucesso do método exponencial sofreu mudança com o aumento de testemunhas exagerando positivamente. Neste caso, o método foi beneficiado, tendo em vista que os exageros positivos o ajudaram a reduzir os maus julgamentos causados por sua convergência exagerada.



(a) (b)

Figura 5.83: Exagero Positivo - Percentual de Tentativas de Sucesso

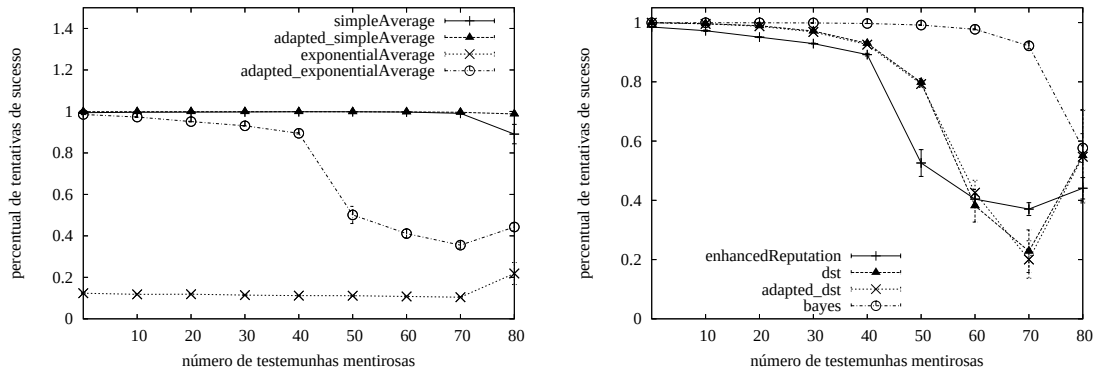
A figura 5.84 mostra as curvas de perda dos métodos nas simulações que consideraram a presença de testemunhas aplicando o ataque do exagero negativo. Como já havia sido estudado, este ataque exerce maior influência nos métodos. O aumento das testemunhas mentirosas causou um crescimento no desperdício de interações de todos os métodos, demonstrando a dificuldade dos clientes em identificarem os provedores bem comportados.



(a) (b)

Figura 5.84: Exagero Negativo - Percentual de Interações Perdidas

A figura 5.85 mostra que, com o aumento de mentirosos exagerando negativamente, os clientes apresentaram dificuldades de organizar suas listas e passaram a fazer mais tentativas em busca do recurso desejado. Nas simulações com um número muito alto de mentirosos, o percentual de sucesso elevou um pouco porque os clientes deixaram, prematuramente, de fazer tentativas, assumindo todos os provedores como mal comportados.



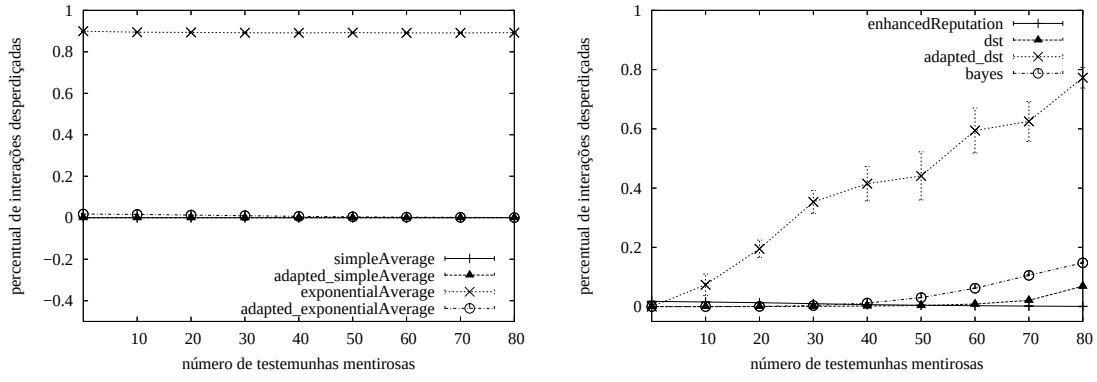
(a) (b)

Figura 5.85: Exagero Negativo - Percentual de Tentativas de Sucesso

A figura 5.86 mostra as curvas de perda dos métodos nas simulações que consideraram a presença de testemunhas aplicando o ataque da mentira complementar. Como foi mencionado anteriormente, neste modelo, enquanto uma testemunha mentirosa não possui experiência a respeito de um provedor, ela fornece informações de segunda mão muito próximas das que realmente calculou (período de honestidade acidental).

Tendo em vista que, neste cenário, os clientes escolhem seus próprios provedores, eles podem acumular experiências com alguns provedores e nem chegar a interagir com outros. Assim, ainda que o número de testemunhas mentirosas na rede seja alto, um cliente pode consultar testemunhas mentirosas que têm experiências suficientes para aplicar a mentira e outras testemunhas, igualmente mentirosas, que ainda estão no período de honestidade acidental com o provedor de interesse do cliente.

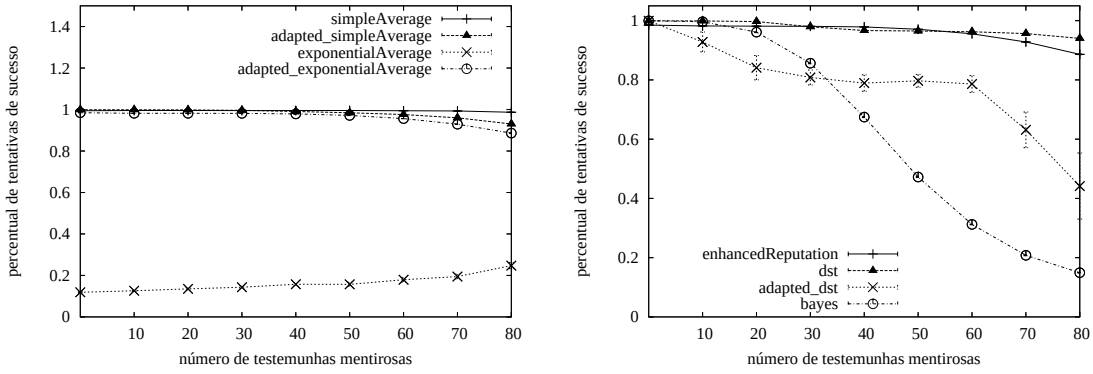
Isso faz com que a maior parte dos métodos apresentem baixo percentual de desperdícios de interações. A única exceção, o método dst adaptado, apresenta um percentual de perda crescente pois, com este método, basta que uma testemunha consultada informe certeza absoluta em hipótese contrária à do cliente que a consultou para que as crenças resultantes a partir da regra de combinação de Depster-Shafer seja 0/0.



(a) (b)

Figura 5.86: Mentira Complementar - Percentual de Interações Perdidas

A figura 5.87 mostra que, além do método dst adaptado, o método Bayesiano sofre uma queda em seu percentual de tentativas de sucesso, demonstrando que os clientes desorganizam um pouco suas listas e precisam fazer mais de uma tentativa para obterem o recurso desejado.

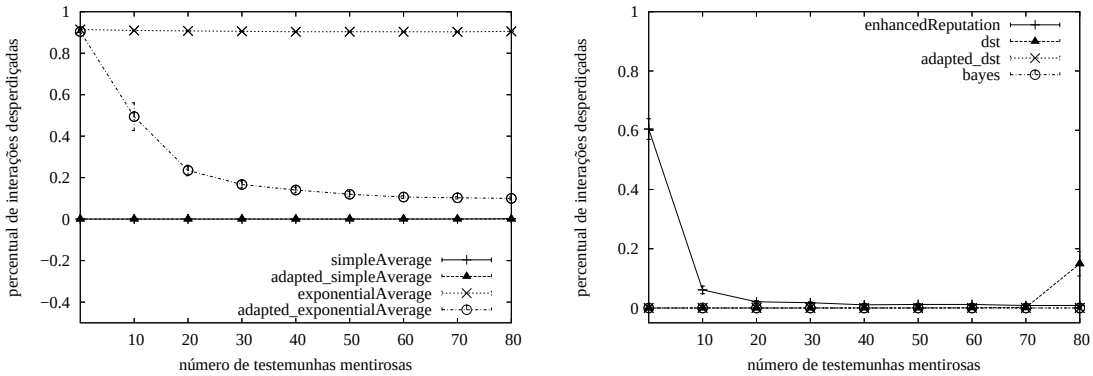


(a) (b)

Figura 5.87: Mentira Complementar - Percentual de Tentativas de Sucesso

A figura 5.88 mostra as curvas de perda dos métodos resultantes de mais uma rodada de simulações que consideraram a presença de testemunhas aplicando o ataque da mentira complementar. Nestas simulações, os clientes foram configurados de maneira a manterem suas próprias listas de testemunhas ordenadas por credibilidade. O método de credibilidade utilizado foi o Bayesiano, que foi configurado com $d = 0.3$ e $\rho = 1$.

A cada interação, o cliente escolhido para interagir consultará sua lista de testemunhas e escolherá aquelas com maiores valores de credibilidade às quais requisitará informações de segunda mão a respeito dos provedores de sua lista de provedores. Depois que este cliente interagir e avaliar o provedor que escolheu, ele atualizará os valores de credibilidade. Se este cliente fizer mais de uma tentativa de conseguir o recurso desejado, os valores de credibilidade serão atualizados depois de cada tentativa.



(a) (b)

Figura 5.88: Lista de Testemunhas Gerenciáveis - Percentual de Interações Perdidas

Comparando a figura 5.88(a) com a 5.86(a), nota-se que a adoção do mecanismo de credibilidade causou bastante perda de desempenho no método exponencial adaptado. Além disso, é possível perceber que os maiores percentuais de desperdícios aconteceram nas simulações que consideraram menores quantidades de testemunhas mentirosas.

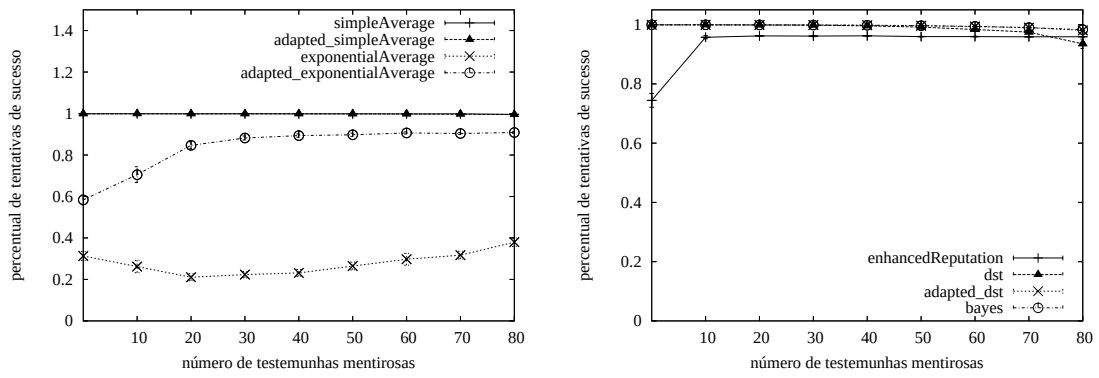
Conforme foi visto, a reputação de primeira mão calculada pelos métodos exponenciais converge muito rápido. Se o método converge rápido demais, os clientes se tornam muito susceptíveis a maus julgamentos de provedores bem comportados. A atualização dos valores de credibilidade é resultado da comparação da experiência vivida pelo cliente com as informações recebidas das testemunhas. Sendo assim, as testemunhas que estiverem julgando mal os provedores bem comportados, serão julgadas como desonestas pelos clientes a quem fornecerem estas informações errôneas.

Foi visto ainda, ao longo do estudo do Cenário 6, que no caso do método exponencial adaptado, quando o cliente associa baixas credibilidades às reputações de suas testemunhas, o valor da reputação tende a $\alpha * R(P_i, P_j)$, valor ainda mais baixo que o calculado a partir de suas experiências próprias. Enfim, neste método, a rápida convergência leva aos maus julgamentos, que leva à queda nos valores de credibilidade, que colabora ainda mais para os maus julgamentos.

A redução nas perdas deste método quando o número de testemunhas mentirosas cresce na rede ocorre porque uma testemunha mentirosa que pratique a mentira complementar informa o contrário do que calculou. Assim, os clientes que estiverem julgando mal os provedores bem comportados, acabarão acertando quando informarem o oposto do que calcularam. Isso reduzirá a velocidade com que os valores de credibilidade cairão. Os valores de credibilidade mais altos, quando considerados pela equação 3.4 deixarão, por sua vez, de colaborar para o cálculo de baixos valores de reputação.

A figura 5.88(b) mostra que o método exponencial sem histórico também sofre com a adoção do mecanismo de credibilidade. Entretanto, o fato deste método trabalhar no intervalo $[-1, 1]$ colabora para que ele não seja afetado da mesma maneira. Já o uso do método de Bayesiano de credibilidade em conjunto com os métodos que usam Dempster-Shafer e Bayes resultaram em bons desempenhos, resultados esperados em virtude do estudo destas combinações no Cenário 6.

Por fim, complementando esta análise, a figura apresenta o percentual de tentativas de sucesso obtidos pelos métodos nesta última rodada de simulações.



(a) (b)

Figura 5.89: Lista de Testemunhas Gerenciáveis - Percentual de Tentativas de Sucesso

5.8 Resumo dos Principais Aspectos Analisados

As simulações executadas nos diferentes cenários possibilitaram verificar algumas características bastante marcantes nos oito métodos estudados.

Os métodos de média simples mostraram melhores desempenhos quando foram utilizados com históricos de tamanho 10. As simulações com históricos de 100 mostraram uma diminuição na velocidade de convergêcia dos métodos, que acabou por prejudicá-los.

As simulações do cenário 4 mostraram que estes métodos praticamente não foram afetados pelo modelo de mentira exagero positivo. O exagero negativo e a mentira complementar conseguiram reduzir o desempenho do método de média simples adaptado, mas influenciaram bem menos o método original, pois este deixa de usar as informações de segunda mão quando os históricos estão cheios.

O método exponencial original demostrou ser muito influênciado por seu parâmetro de fator de decaimento. O método exponencial adaptado e o sem histórico, por se manterem usando as informações de segunda mão, apresentaram desempenhos bem melhores que o método exponencial original ao longo das simulações.

O cenário 3 mostrou que a velocidade de convergência dos métodos exponencial adaptado e sem histórico fizeram com que eles detectassem, antes dos demais mecanismos testados, a mudança brusca de comportamento do *peer* que estava se comportando bem até a metade das simulações e depois passou a se comportar mal. Esta vantagem só foi perdida quando um valor muito baixo de fator de decaimento foi adotado, pois, desta maneira,

reduzi-se muito a convergência de tais métodos.

Estes dois métodos mostraram-se bastante dependentes do uso das informações de segunda mão. Como possuem um cálculo de primeira mão que converge muito rápido, o número de maus julgamentos tendem a aumentar em ambos os mecanismos se um baixo peso ou um peso nulo é associado às informações de segunda mão.

As simulações do cenário 4 mostraram que os métodos exponenciais praticamente não foram afetados pelo modelo de mentira exagero positivo. Já o exagero negativo e a mentira complementar reduziram o desempenho tanto do método exponencial adaptado quanto do sem histórico.

Os métodos que usam a teoria de Dempster-Shafer demostraram que são muito afetados pelo uso de históricos grandes, de tamanho 100. Utilizando históricos de tamanho 10, estes métodos apresentaram excelente capacidade de identificação de provedores bem e mal comportados durante as simulações do cenário 1.

Além disso, o estudo destes métodos no cenário 2 demonstrou que a utilização da regra de combinação de Dempster-Shafer, que trabalha de maneira explícita com a incerteza, realmente proporcionou uma vantagem em cenários onde os clientes cometem falhas de avaliação. O método dst adaptado atingiu um desempenho melhor do que todos os métodos, inclusive melhor que o obtido pelo método dst original, que pára de usar a regra de Dempster-Shafer depois do preenchimento dos seus históricos.

As simulações do cenário 4 mostraram que estes mecanismos praticamente não foram afetados pelo modelo de mentira exagero positivo, enquanto que o exagero negativo reduziu consideravelmente seus desempenhos. O modelo de mentira complementar também diminuiu bastante o desempenho de ambos e demonstrou um problema na utilização da regra de combinação de Dempster-Shafer: as crenças resultam em 0/0 quando a regra de combinação de Dempster-Shafer é usada para combinar crenças que expressam absoluta certeza em hipóteses contrárias.

O método Bayesiano apresentou resultados bastante satisfatórios nos cenários considerados. Este método tem somente um parâmentro a ser configurado, a constante u, que proporciona o efeito de decaimento do peso das informações de primeira mão mais antigas. O bom desempenho conseguido por este mecanismo no cenário 1 não foi afetado pela variação deste parâmentro.

Já no cenário 2, que considerou um ambiente de incerteza, valores mais baixos desta

variável foram necessários para garantir um desempenho mais adequado ao mecanismo. O mesmo aconteceu no cenário 3, onde valores reduzidos de u foram usados para tornar possível a detecção da brusca mudança de comportamento do *peer* que deixou de ser bem comportado no meio da simulação.

As simulações do cenário 4 mostram que o mecanismo de Bayes foi afetado por todos os modelos de mentira. No caso do exagero positivo, menores valores associados a u ajudaram o método a aumentar seu desempenho. Entretanto a redução do valor deste parâmentro não o afeta significativamente quando os modelos de mentira são exagero negativo ou mentira complementar.

Com relação aos mecanismos de credibilidade testados no cenário 6, o WMA não demostrou ser uma boa opção de uso. Este método faz com que os clientes não aumentem os valores de credibilidade para as suas testemunhas quando as mesmas acertam em suas recomendações, mas causa a redução de seus valores de credibilidade para quaisquer diferença entre as informações de segunda mão oferecidas pelas testemunhas e a experiência vivida pelo cliente que as requisitou.

A queda inevitável no valor das credibilidades causa perda de desempenho na maior parte dos métodos. Somente os métodos dst, dst adaptado e bayes conseguem aumentar seus desmpenhos com a utilização deste método, que causa o desprezo das informações de segunda mão depois de algumas interações.

As simulações com o método Bayesiano de credibilidade demostraram que, quando o teste de desvio utilizado por ele é configurado de maneira a não ser tão rigoroso (d = 0.3), este mecanismo pode proporcionar aos clientes mais justiça no momento do julgamento das testemunhas. Testemunhas que não passarem no teste do desvio terão seus valores de credibilidade reduzidos, mas ao contrário do que acontece no WMA, elas poderão ter sua credibilidade aumentada caso acertem em suas recomendações.

O cenário 7 testou todos os métodos em diferentes cenários no modo de simulação com lista de provedores gerenciável. A maioria dos resultados obtidos confirmaram os estudos que já tinham sido feitos no modo de provedor definido. A simulação final, que considerou clientes escolhendo seus próprios provedores e suas próprias testemunhas em um cenário com *peers* executando o ataque da mentira complementar, demonstrou que o uso do mecanismo Bayesiano de credibilidade só demonstrou ser uma vantagem para os métodos dst, dst adaptado e bayes.

Capítulo 6

Conclusões

6.1 Contribuições

Este trabalho estudou oito mecanismos de incentivo à cooperação baseados em reputação testando-os em diversos cenários no simulador desenvolvido em C para este fim. Sua principal contribuição foi a comparação justa de diversos métodos matemáticos de cálculo de reputação, que foram testados sob as mesmas condições.

Além de simular os métodos em cenários de baixa complexidade, compostos apenas por *peers* bem e mal comportados, o simulador permitiu montar ambientes mais elaborados. Os métodos foram testados em ambientes de incerteza, onde os clientes tinham a possibilidade de falhar no momento de avaliar seus provedores.

Em muitas simulações foram considerados ambientes hostis, que continham *peers* maliciosos atacando os mecanismos de reputação (mudança repentina de comportamento e ataque do testemunho mentiroso). Outros cenários consideraram mecanismos de reputação trabalhando em conjunto com mecanismos de credibilidade. Dois mecanismos de credibilidade foram testados e seus desempenhos comparados.

A medida que os cenários simulados aumentavam de complexidade, os resultados permitiam um estudo mais aprofundado dos métodos e eram revelados seus pontos fortes e fracos. Outras importantes contribuições deste trabalho foram as propostas de três métodos, resultantes de adaptações executadas em três propostas da literatura: o método de média simples adaptado, o método exponencial adaptado e o método dst adaptado.

Por fim, uma importante contribuição foi o desenvolvimento do simulador, que pode ser usado como ferramenta para o testes de outras propostas de mecanismos de reputação

e/ou de mecanismos de credibilidade, além de poder ter sua implementação alterada de forma a testar outros cenários e outros ataques aos mecanismos de reputação.

6.2 Trabalhos Futuros

A implementação do simulador em C possibilita um bom número de trabalhos futuros. Como principal indicamos a utilização de todo o conhecimento ganho no estudo dos mecanismos estudados para o desenvolvimento de uma nova proposta de mecanismo que tente reunir o máximo de vantagens apresentadas pelos métodos.

Outra possibilidade de trabalho futuro é a avaliação de outras propostas de mecanismos de credibilidade, que possibilite aos métodos maiores ganhos em ambientes onde o ataque do testemunho mentiroso esteja sendo executado.

Outro caminho seria o estudo de diferentes modelos de cenários, que aproximassem cada vez mais os ambientes gerados dos reais, encontrados nos principais softwares P2P, como nos softwares de compartilhamento de arquivos Gnutella e Napster.

6.3 Considerações Finais

O Capítulo 5 apresentou os resultados obtidos a partir das simulações dos oito métodos, apresentados no Capítulo 3, em diferentes cenários. A análise de tais resultados demonstrou que os desempenhos dos métodos nos cenários considerados são bastante dependentes dos valores associados aos parâmetros específicos de cada mecanismo.

Nenhum dos métodos estudados foi melhor em todos os cenários analisados. Assim, a escolha de algum destes métodos de reputação por um desenvolvedor de aplicação P2P irá requerer um estudo do perfil de seus usuários. A grande questão é que, em se tratanto de redes P2P onde usuários conectam e desconectam da rede o tempo todo, este perfil pode não ser estável. Se o perfil de usuários variar muito e o desenvolvedor não conseguir nem mesmo traçar uma tendência, a adoção de um mecanismo de reputação poderia até mesmo atrapalhar o desempenho da rede em determinadas ocasiões.

Sendo assim, o simulador torna-se uma ferramenta essencial para que novas propostas de novos métodos, ou talvez de mecanismos adaptativos, tentem sanar este problema, garantindo bons desempenhos nos mais diversos cenários.

Referências Bibliográficas

[1] LIANG, J., KUMAR, R., ROSS, K., "The Kazaa Overlay: A Measurement Study". In: *Proceedings of the 19th IEEE Annual Computer Communications Workshop*, Florida, EUA, outubro 2004.

[2] "KaZaA", `http://www.kazaa.com`, visitado em 18 de outubro de 2008.

[3] SAROIU, S., GUMMANDI, P. K., GRIBBLE, S. D., "A measurement study of peer-to-peer file sharing systems". In: *Proceedings of Multimedia Computing and Networking (MMCN 02)*, San Jose, CA, EUA, 2002.

[4] ADAR, E., HUBERMAN, B., "Free riding on gnutella", http://www.hpl.hp.com/research/idl/papers/gnutella, visitado em 18 de outubro de 2008.

[5] ASVANUND, A., CLAY, K., KRISHNAN, R., et al., "An Empirical Analysis of Network Externalities in Peer-to-Peer Music-Sharing Networks", *Information Systems Research*, v. 15, n. 2, pp. 155–174, 2004.

[6] HUGHES, D., COULSON, G., WALKERDINE, J., "Free Riding on Gnutella Revisited: The Bell Tolls?" *IEEE Distributed Systems Online*, v. 6, n. 6, pp. 1, 2005.

[7] LIU, J., ISSARNY, V., "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks". In: *Proceedings of iTrust 2004*, pp. 48–62, Oxford, UK, 2004.

[8] BUCHEGGER, S., BOUDEC, J.-Y. L., "A Robust Reputation System for P2P and Mobile Ad-hoc Networks". In: *Second Workshop on Economics of Peer to Peer Systems*, Harvard University, Cambridge, MA, 2004.

[9] WANG, Y., “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)*, Melbourne, Australia, 2003.

[10] WANG, Y., VASSILEVA, J., “Trust and reputation model in peer-to-peer networks”. In: *Proceedings of Third International Conference on Peer-to-Peer Computing, 2003. (P2P 2003)*, Washington, EUA, 2003.

[11] YU, B., SINGH, M., “Detecting Deception in Reputation Management”. In: *Proceedings of the Second International Joint Conference on Autonomous Agents and Multi Agent Systems (AAMAS03)*, Melbourne, Australia, 2003.

[12] YU, B., SINGH, M., “An Evidential Model of Distributed Reputation Management”. In: *Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, Bologna, Italy, 2002.

[13] YU, B., SINGH, M., SYCARA, K., “Developing Trust in Large Scale Peer-to-Peer Systems”. In: *Proceedings of First IEEE Symposium on Multi-Agent Security and Survivability*, Philadelphia, PA, 2004.

[14] ROCHA, J., DOMINGUES, M., CALLADO, A., et al., “Peer-to-Peer: Computação Colaborativa na Internet”. In: *22º Simpósio Brasileiro de Redes de Computadores - SBRC2004 (minicurso)*, Gramado, RS, 2004.

[15] “ICQ”, `http://www.icq.com/`, visitado em 18 de outubro de 2008.

[16] “MSN”, `http://im.live.com/Messenger/IM/Home`, visitado em 18 de outubro de 2008.

[17] “Yahoo! Messenger”, `http://messenger.yahoo.com/`, visitado em 18 de outubro de 2008.

[18] PICARD, P., “Risk Exposure: Instant Messaging and Peer-to-Peer Networks v2.0”, http://security.ittoolbox.com/white-papers/risk-exposure-through-instant-messaging-and-peertopeer-p2p-networks-3441, 2003.

[19] LUNDGREN, H., GOLD, R., NORDSTRÖM, E., et al., “A Distributed Instant Messaging Architecture based on the Pastry Peer-to-Peer Routing Substrate”. In: *Swedish National Computer Networking Workshop 2003 (poster)*, Stockholm, 2003.

[20] YANG, B., GARCIA-MOLINA, H., *Comparing hybrid peer-to-peer systems (extended)*, Tech. rep., 2000.

[21] RIPEANU, M., FOSTER, I., IAMNITCHI, A., “Mapping the gnutella network: Properties of large-scale peer-to-peer systems and implications for system design”, *IEEE Internet Computing Journal*, v. 6, n. 1, 2002.

[22] DAMIANI, E., DI VIMERCATI, D. C., PARABOSCHI, S., et al., “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*, Washington, DC, EUA, 2002.

[23] NANDI, A., NGAN, T.-W., SINGH, A., et al., “Scrivener: Providing Incentives in Cooperative Content Distribution Systems”. In: *ACM/IFIP/USENIX 6th International Middleware Conference (Middleware 2005)*, Grenoble, França, 2005.

[24] ASVANUND, A., BAGLA, S., KAPADIA, M. H., et al., “Intelligent Club Management in Peer-to-Peer Networks”. In: *Proceedings of First Workshop on Economics of Peer to Peer Systems*, Berkeley, CA, 2003.

[25] SURYANARAYANA, G., DIALLO, M. H., ERENKRANTZ, J. R., et al., “Architecting trust-enabled peer-to-peer file-sharing applications”, *Crossroads*, v. 12, n. 4, 2006.

[26] “Napster”, `http://www.napster.com/`, visitado em 18 de outubro de 2008.

[27] “Gnutella”, `http://www.gnu.org/philosophy/gnutella.html`, visitado em 18 de outubro de 2008.

[28] “FreeNet”, `http://freenetproject.org/`, visitado em 18 de outubro de 2008.

[29] LUA, K., CROWCROFT, J., PIAS, M., et al., “A survey and comparison of peer-to-peer overlay network schemes”, *Communications Surveys & Tutorials, IEEE*, pp. 72–93, 2005.

[30] T, K., O, K., J, K., et al., “Peer-to-Peer Community Management using Structured Overlay Networks”. In: *Proceedings of International Conference on Mobile Technology, Applications and Systems*, Taiwan, 2008.

[31] VISHNUMURTHY, V., CHANDRAKUMAR, S., SIRER, E., “KARMA: A Secure Economic Framework for Peer-to-Peer Resource Sharing”. In: *Proceedings of First Workshop on Economics of Peer to Peer Systems*, Berkeley, CA, 2003.

[32] GOLLE, P., LEYTON-BROWN, K., MIRONOV, I., “Incentives for Sharing in Peer-to-Peer Networks”. In: *Proceedings of the Third ACM Conference on Electronic Commerce*, Tampa, Florida, EUA, 2001.

[33] BUTTYAN, L., HUBAUX, J. P., “Enforcing Service Availability in Mobile Ad-Hoc WANs”. In: *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc)*, ACM Press: Boston, 2000.

[34] BUTTYAN, L., HUBAUX, J. P., *Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks*, Tech. Rep. Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, 2001.

[35] BUTTYAN, L., HUBAUX, J. P., “Stimulating Cooperation in Self-Organizing Mobile Ad-Hoc Networks”. In: *ACM Journal for Mobile Networks (MONET), Special Issue on Mobile Ad Hoc Networking*, v. 8, 2002.

[36] MARTI, S., GIULI, T. J., LAI, K., et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”. In: *Proceedings of Sixth Annual International Conference on Mobile Computing and Networking*, pp. 255–265, ACM Press: Boston, 2000.

[37] MICHIARDI, P., MOLVA, R., “Simulation-Based Analysis of Security Exposure in Mobile Ad Hoc Network”. In: *Proceedings of the Mobile Ad Hoc Networks European Wireless Conference*, 2002.

[38] ROCHA, L. G. S., COSTA, L. H. M. K., DUARTE, O. C. M. B., “Analyzing the Impact of Misbehaving Nodes in Ad Hoc Routing”. In: *The 3rd IEEE Latin American Network Operations and Management Symposium - LANOMS’2003*, pp. 5–12, Foz do Iguaçu, Brazil, 2003.

[39] “eBay”, `http://www.ebay.com/`, visitado em 18 de outubro de 2008.

[40] JØSANG, A., ISMAIL, R., BOYD, C., “A Survey of Trust and Reputation Systems for Online Service Provision”. In: *Decision Support Systems*, v. 43, n. 2, Elsevier Science Publushers B. V., 2007.

[41] BUCHEGGER, S., BOUDEC, J.-Y. L., “Performance Analisys of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)”. In: *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Lausanne, Suiça, 2002.

[42] MICHIARDI, P., MOLVA, R., “CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks”. In: *Proceedings of the Sixth IFIP Conference on Security, Communications, and Multimedia (CSM 2002)*, Portoroz, 2002.

[43] BUCHEGGER, S., BOUDEC, J.-Y. L., “The Effect of Rumor Spreading in Reputation Systems for Mobile Ad Hoc Networks”. In: *Proceedings of WiOpt 2003*, pp. 131–140, Sophia-Antipolis, 2003.

[44] BUCHEGGER, S., BOUDEC, J.-Y. L., “Self-policing mobile ad-hoc networks by reputation systems”, *IEEE Communications Magazine*, v. 43, n. 7, 2005.

[45] HE, Q., WU, D., KHOSLA, P., “SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks”. In: *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2004)*, v. 2, pp. 825–830, Atlanta, GA, EUA, 2004.

[46] J. MUNDINGER, J.-Y. L. B., “Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars”. In: *Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt’05)*, pp. 41–46, Trento, Italy, 2005.

[47] MORTAZAVI, B., KESIDIS, G., “Cumulative Reputation Systems for Peer-to-Peer Content Distribution”. In: *40th Annual Conference on Information Sciences and Systems*, 2006.

[48] JUN, S., AHAMAD, M., “Incentives in BitTorrent induce free riding”. In: *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems (P2PECON05)*, Philadelphia, Pennsylvania, USA, 2005.

[49] RODRIGUEZ-PEREZ, M., ESPARZA, O., JOSE L. MU N., “Surework: a super-peer reputation framework for p2p networks”. In: *Proceedings of the 2008 ACM symposium on Applied computing (SAC08)*, Fortaleza, Ceara, Brazil, 2008.

[50] ABDUL-RAHMAN, A., HAILES, S., “Supporting Trust in Virtual Communities”. In: *Proceedings of the 33th Hawaii International Conference on System Sciences*, Maui, Hawaii, 2000.

[51] SENTZ, K., *Combination of Evidence in Dempster-Shafer Theory*, Ph.D. Thesis, SNL, LANL, and Systems Science and Industrial Eng. Dept., Binghamton Univ, 2002.

[52] YU, B., SINGH, M., “Distributed Reputation Management for Eletronic Commerce”. In: *Computational Intelligence*, v. 18, n. Issue 4, pp. 535–549, 2002.

[53] MUI, L., MOHTASHEMI, M., HALBERSTADT, A., “A Computational Model of Trust and Reputation”. In: *Proceedings of the 35th Hawaii International Conference on System Sciences*, Maui, Hawaii, 2002.

[54] JØSANG, A., HIRD, S., FACCER, E., “Simulating the Effect of Reputation Systems on e-Markets”. In: *Proceedings of First International Conference on Trust Management*, Grécia, 2003.

[55] FELDMAN, M., CHUANG, J., “Overcoming free-riding behavior in peer-to-peer systems”, *SIGecom Exch.*, v. 5, n. 4, pp. 41–50, 2005.

[56] DEWAN, P., DASGUPTA, P., “Securing P2P networks using peer reputations: is there a silver bullet?” In: *Proceedings of Consumer Communications and*

Networking Conference, 2005 (CCNC 2005), pp. 30–36, Tempe, AZ, EUA, 2005.

[57] XU, P., GAO, J., GUO, H., "Rating Reputation: A Necessary Consideration in Reputation Mechanism". In: *Proceedings of 2005 International Conference on Machine Learning and Cybernetics, 2005*, China, 2005.

[58] PAUL, K., WESTHOFF, D., "Context Aware Inferencing to Rate a Selfish Node in DSR Based Ad Hoc Networks". In: *Proceedings of the IEEE Globecom Conference*, IEEE: Taipeh, Taiwan, 2002.

[59] DA SILVA, F. M., DE REZENDE, J. F., "Avaliação de Métodos Matemáticos usados nos Modelos de Reputação de Incentivo à Cooperação". In: *Anais do 25º Simpósio Brasileiro de Redes de Computadores (SBRC2007)*, Belém - Pará - Brasil, 2007.

[60] DA SILVA, F. M., DE REZENDE, J. F., "Influência do Ataque do Testemunho Mentiroso nos Modelos de Reputação". In: *Anais do 26º Simpósio Brasileiro de Redes de Computadores (SBRC2008)*, Rio de Janeiro - Brasil, 2008.