HÉLIO MARCOS PAZ DE ALMEIDA

UM MODELO BASEADO EM REPUTAÇÃO E PROTOCOLO DE RUMORES PARA EVITAR ATAQUES SYBIL EM REDES PAR-A-PAR

Belo Horizonte
11 de dezembro de 2006

Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Programa de Pós-Graduação em Ciência da Computação

UM MODELO BASEADO EM REPUTAÇÃO E PROTOCOLO DE RUMORES PARA EVITAR ATAQUES SYBIL EM REDES PAR-A-PAR

Dissertação apresentada ao Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

HÉLIO MARCOS PAZ DE ALMEIDA

Belo Horizonte
11 de dezembro de 2006

UNIVERSIDADE FEDERAL DE MINAS GERAIS

FOLHA DE APROVAÇÃO

Um Modelo Baseado em Reputação e Protocolo de Rumores para Evitar ataques Sybil em Redes Par-a-Par

HÉLIO MARCOS PAZ DE ALMEIDA

Dissertação defendida e aprovada pela banca examinadora constituída por:

Ph. D. Dorgival Olavo Guedes Neto – Orientador

Ph. D. Wagner Meira Jr.
Universidade Federal de Minas Gerais

Ph. D. Virgílio A. F. Almeida
Universidade Federal de Minas Gerais

Belo Horizonte, 11 de dezembro de 2006

Resumo

Sistemas Par-a-Par (*P2P*) utilizam a cooperação entre diversos nós para fornecer seus serviços. Um problema, entretanto, é que é possível que alguns participantes tentem utilizar os recursos fornecidos por outros membros da rede sem disponibilizar em troca seus próprios recursos, um comportamento conhecido como oportunista ou *free-rider*. Uma forma de impedir que usuários ajam de maneira oportunista é utilizar mecanismos de reputação. Nesse tipo de mecanismo, o comportamento dos nós com relação ao fornecimento de serviço é registrado e compartilhado entre os participantes da rede. Com essa informação, um nó bem comportado pode avaliar se é interessante atender a um outro nó que solicita seus recursos com base na reputação atribuída àquele nó. Uma dissertação de mestrado anterior (Bruno Gusmão Rocha, 2005) desenvolveu um mecanismo de reputação baseado em teoria de jogos para combater o comportamento oportunista em uma rede sobreposta de roteamento, com bons resultados.

Contudo, existem problemas que não foram tratados naquele trabalho. Um desses problemas são ataques Sybil, que ocorrem quando um único usuário acessa o sistema utilizando diversas identidades, utilizando-as para obter recursos de forma indevida. Além disso, aquele trabalho utilizava um estado global para calcular a reputação dos participantes, o que limita sua escalabilidade. Ainda, o trabalho foi desenvolvido num ambiente P2P específico (redes de roteamento sobrepostas), mas seria interessante averiguar se o modelo apresentado pode ser utilizado com sucesso em outros ambientes P2P, como no compartilhamento de arquivos.

Nossas alterações do modelo atacaram esses três problemas. Em um primeiro momento, fomos capazes de excluir nós Sybil do modelo de reputação com bom desempenho, sem influenciar negativamente no serviço fornecido a nós justos no modelo original. Além disso, alteramos o modelo original de forma a não exigir a manutenção de um estado global; verificamos que o modelo alterado ainda apresenta resultados próximos aos obtidos originalmente mesmo com essa alteração. Finalmente, aplicamos o modelo de reputações à rede de compartilhamento de arquivos *BitTorrent*, conseguindo uma melhor restrição de serviço fornecido a *free-riders* maliciosos que a rede original.

Abstract

Peer-to-Peer (P2P) systems use the cooperation between the nodes of the system to provide their services. However, it is possible for some participants to use resources provided by other nodes without giving anything back, a behavior known as free-riding. One way to force users not to act as free-riders is to use reputation mechanisms. In such a mechanism, the behavior of nodes in respect to the provision of service to others is recorded and shared among the network nodes. With that information, a fair node can decide whether it should serve another node's request or not, based on the reputation of the requesting node. A previous dissertation (Bruno Gusmão Rocha, 2005) proposed a reputation mechanism based on game theory to exclude free-riders from a routing overlay network with good results.

However, there are some problems that were not addressed by that work. One of those problems are Sybil attacks, which happen when a single user approaches the system with multiple identities, using them to get resources through mischief. Besides, that work required a global state in order to compute the participants reputation, what limits its scalability. Finally, the work was developed with a specific P2P environment in mind (routing overlay networks), but it would be interesting to see if the model could be applied successfully to other P2P systems, like those for file sharing.

Our changes to the model focused those three problems. In a first moment, we were able to exclude Sybil nodes with good performance, without hurting the service provided to fair nodes in the original model. We then altered the model to remove the need for a global state and observed that the new model stil presented performance close to the original model, even after that modification. Finally, we applied the reputation-based model to the BitTorrent file sharing network, achieving a better restriction to free-riders than that of the original network.

A meus pais, por tudo.

Agradecimentos

Agradeço a Deus por todas as oportunidades que tive. A meus pais, Herbert e Fátima, por todo amor e apoio (espero tê-los feito orgulhosos). Ao meu irmão Herbert pelo ano de boa companhia em BH. A meus tios e tias do coração, Yolanda, Gilka, Matos, Petrus, Dida, Alexandre, Amira, Glauco, Eterlene, Eliana, meus padrinhos Reiko e Guilherme, minha "avó" Luísa e suas famílias, que sempre torceram por mim.

Agradeço a minha avó Militina por todas as preces e a meus tios e tias de Brasília, Vera, Ana, Teresa, Calíope, Cristina, Léo e respectivas famílias. Agradeço também à minha família mineira, que me acolheu de braços e corações abertos, sempre ao meu lado nesse lar longe do lar. Gostaria de poder citar todos por nome, mas como o espaço é limitado eu os homenageio em nome de minhas tias Nazi, Alzira, Rosário, Irene e Eneida, e de meus primos Isabela (obrigado por todo o carinho), Hassan e Hamud.

Não posso esquecer também do meu orientador, Dorgival, e do André e do Macambira, um grupo de trabalho totalmente excelente! E aos meus professores da graduação Rodrigo e Carla, pelo apoio que me deram para tentar o mestrado.

E claro que não posso deixar de citar meus amigos, por todo apoio e por estarem sempre ao meu lado, de uma forma ou de outra. A velha guarda em Belém, Mário (um irmão e cão maldito), Marilia (sumida), Nádia (louca), Léo (outro maldito), Pio (pano preto), Rosana (bonito sorriso. Eu tenho um igual :P), Alex e Sueleny. Aos novos amigos de BH, Paulo (valeu por tudo, "sô"), Denise (não mude nunca), Ana (apesar da implicância) e Nathalia (minha linda, ainda não acredito na sorte que eu tenho). E às minhas primas adotivas Izabela, Verena e Letícia, lá de Belém, e Carol, Nina (os pompons foram mesmo um charme à parte) e Ellen, aqui de BH.

Sem vocês eu não teria conseguido chegar onde estou. E mesmo se conseguisse, não teria a menor graça!

Sumário

Lista de Figuras

Capítulo 1

Introdução

Redes Par-a-Par (P2P) requerem uma quantia significativa de cooperação entre seus elementos para de fato alcançarem todo seu potencial. Entretanto, tal cooperação nem sempre é facilmente obtida. Considerando que os elementos de uma rede possuem um comportamento egoísta (ou seja, buscam melhores resultados para si, desconsiderando o bem global), pode ser mais interessante para eles tentar utilizar os recursos alheios sem fornecer seus próprios recursos a outros. Um elemento com tal comportamento é chamado de oportunista (*freerider*).

Para evitar esse tipo de comportamento pode-se utilizar mecanismos de reputação. Nesse tipo de mecanismo um nó A decide se fornece ou não serviços a outro nó B baseado em suas experiências anteriores com ele, além da opinião geral dos outros nós participantes da rede em relação a B. Para tal é necessário que haja a disseminação das informações de reputação de cada nó para todos os outros nós da rede.

Um mecanismo baseado em reputação para lidar com oportunistas foi desenvolvido por Rocha [32]. Nele cada nó foi modelado como um participante de um jogo não cooperativo cujo objetivo é realizar conexões com seus vizinhos de modo a maximizar algum benefício específico, como por exemplo menor latência. A cada interação entre dois nós a experiência individual entre eles é alterada, aumentado em caso de sucesso e diminuindo em caso de falha. Os valores de experiência individual diminuem com maior velocidade do que aumentam, de modo a inibir comportamento oportunista. Além disso, todos os nós que entram no sistema são considerados "inocentes" e cada nó possui um limite mínimo de valor de reputação diferente para aceitar requisições, de modo que um nó justo que sofra algum problema e não possa responder a algumas requisições ainda poderá se comunicar com parte dos nós da rede e assim compensar as suas falhas.

Rocha apresenta bons resultados na identificação e negação de serviços a oportunistas sem interferir no serviço fornecido a nós justos. Porém, aquele trabalho con-

sidera que cada oportunista apresenta apenas um comportamento egoísta, isto é, os nós agem individualmente. Se ele apresentasse um comportamento *malicioso* (ou seja, tentar ativamente obter benefícios utilizando-se de métodos escusos), o comportamento do sistema pode não ser tão bom.

Para burlar mecanismos de reputação, um participante pode realizar um ataque Sybil [18]. Esse ataque consiste em um elemento participar da rede utilizando várias identidades diferentes. Dessa forma cada uma das identidades Sybil (como são chamadas as identidades falsas) pode informar à rede que as outras são justas, confundindo assim o sistema de reputações.

Dessa forma, neste trabalho observaremos o comportamento do sistema em face a um ataque Sybil, que consiste em um atacante acessar uma rede usando várias identidades virtuais, possibilitando dessa forma realizar sozinho outros tipos de ataques a uma rede que exijam conluio entre mais de um participante da rede.

Além disso, no modelo de Rocha cada nó necessita de informações de reputação de todos os outros nós da rede, processo esse que requer $O(n^2)$ mensagens, que não é problema num ambiente de redes de roteamento, mas pode ser excessivo em outros tipos de aplicações P2P. Portanto, defendemos o uso de um protocolo de disseminação não instantânea de informação conhecido como protocolo de rumores (*gossip*) [16], que tem por característica uma disseminação de informação menos agressiva, aplicado ao modelo proposto com Rocha, de modo a permitir maior escalabilidade a ele.

Finalmente, o trabalho de Rocha trata do problema de nós oportunistas em um ambiente de redes sobrepostas de roteamento [2]. Todavia, outras aplicações em redes P2P também apresentam problemas com usuários oportunistas, especialmente as redes de compartilhamento de arquivos como Gnutella [31], Kazaa [26] e BitTorrent [11]. Nesse sentido, neste trabalho adaptamos o modelo de Rocha para aplicá-lo a esse novo ambiente, especificamente na obtenção de arquivos e escolha de fontes na rede BitTorrent, para coibir o comportamento oportunista de nós.

1.1 Contribuições

As principais contribuições deste trabalho são:

- apresentação de um estudo detalhado do comportamento do modelo baseado em reputação apresentado por Rocha.
- adaptação desse modelo para lidar de forma mais adequada com ataques Sybil;
- adaptação do modelo para o uso de um protocolo de rumores para que haja uma manutenção menos agressiva do estado global exigido nele;

- aplicação do modelo em um ambiente diferente daquele para o qual ele foi criado (nesse caso, numa rede de compartilhamento de arquivos.

1.2 Trabalhos relacionados

Os trabalhos relacionados estão divididos e quatro categorias: trabalhos relacionados a mecanismos de reputação e teoria dos jogos, trabalhos que tratam de ataques Sybil, trabalhos que utilizam protocolos de rumores e trabalhos que tratam do protocolo da rede *BitTorrent*.

1.2.1 Modelos de reputação e teoria de jogos

Além do trabalho de Rocha [32], outros trabalhos já utilizaram a teoria de jogos e mecanismos de reputação para garantir confiabilidade e justiça em redes P2P. Fabrikant apresentou um modelo para criação desse tipo de rede utilizando teoria de jogos [19] . O protocolo CONFIDANT [7] utiliza o conceito de reputação para decidir o caminho utilizado por pacotes enviados. Alguns trabalhos foram realizados para aumentar a robustez desse sistema, como utilizar informações de vizinhos para calcular reputação [9], evitar falsas acusações [8] e falsos elogios [10]. Este último utiliza um mecanismo probabilístico para excluir nós que emitem falsos elogios, mas ainda não trata ataques Sybil. Gollapudi utiliza teoria de jogos para modelar um sistema de alocação de banda em [35], mas também não trata ataques Sybil. Os sistemas CREDENCE [39] e EigenTrust [24] utilizam reputação para identificar poluição (compartilhamento de conteúdo falso ou adulterado) em redes P2P de compartilhamento de arquivos.

1.2.2 Ataques Sybil

A defesa contra ataques Sybil pode ser feita de duas formas: utilizando-se uma entidade centralizada confiável para certificar os participantes ou de forma descentralizada. Considerando o escopo voltado a redes P2P deste trabalho, focaremos nossa atenção a soluções que não dependam de uma entidade centralizada confiável. Douceur [18] sugere que cada nó valide os outros passando "tarefas" complexas simultaneamente para eles. Estas tarefas deveriam ser complexas de forma que se uma entidade possuísse mais de uma identidade, ela não seria capaz de realizar todas as tarefas no tempo determinado. Identidades que não respondessem à tarefa no tempo determinado pelo requisitante seriam consideradas forjadas. Porém, considerando a grande heterogeneidade de hardware dos participantes de uma rede P2P, torna-se difícil considerar um tempo médio para o término das tarefas sem ser injusto com possíveis usuários justos,

mas com menos recursos. Outros trabalhos tratam do Sybil em ambientes de redes de sensores sem fio [27]. Todavia, esses ambientes possuem muitas especificidades (como, por exemplo, a possibilidade de assinalamento de chaves criptográficas a cada nó antes da inicialização da rede) e portanto soluções aplicáveis a eles dificilmente seriam factíveis em ambientes de redes tradicionais.

Um trabalho que trata o problema do ataque Sybil num ambiente que utiliza reputações é o de Seigneur [37]. Nele, toda vez que um nó precisa de um serviço, ele procura outro nó que possa servir de intermediador da transação. O intermediador escolhe algum nó que ele confia e o sugere ao requisitante, sacrificando parte da sua reputação no processo. Essa reputação que o intermediador sacrifica não é compensada mesmo que transação entre os dois outros nós tenha sucesso. Sem um mecanismo de incentivo é possível que mesmo nós justos, mas egoístas, simplesmente decidam não intermediar nenhuma transação.

Também existem trabalhos que tratam do ataque Sybil em tabelas hash distribuídas (como a rede CHORD [38]). Dinger [17] trata o ataque Sybil através do processo de registro de novos nós na rede, tentando assim impedir que nós Sybil entrem na rede. Nesse trabalho, cada identidade que tenta participar da rede precisa anteriormente se registrar com alguns nós e esses nós avaliam se o identificador externo daquele nó (o endereço IP) combina com o identificador que ele apresenta para participar da rede (que é obtido aplicando uma função *hash* ao identificado externo), além de verificar se essa combinação já está presente na rede. Já Danezis [14] tenta diminuir o efeito de nós Sybil que tentem atrapalhar o processo de roteamento de buscas na rede guardando a informação de quais nós rotearam buscas adequadamente. Dessa forma, ele passa a alternar as mensagens de busca, ora para um nó que ele considere mais próximo do destino, ora para um nó que ele acredite que seja confiável, de forma a sempre usar a informação de um nó confiável para localizar nós mais próximos ao alvo da busca.

1.2.3 Protocolos de rumores

Protocolos de rumores são utilizados em diversos tipos de aplicações para a manutenção de um estado global consistente entre os nós. Por exemplo, sistemas de banco de dados [16], redes de sensores [25], *publish-subscribe* [12] e redes *ad-hoc* móveis [15] utilizam protocolos *gossip* com sucesso na disseminação de informações.

1.2.4 *BitTorrent*

A rede P2P de compartilhamento de arquivos *BitTorrent* [11] tem vários trabalhos que buscam avaliar o seu comportamento utilizando dados reais do compartilhamento de

um arquivo. Pouwelse [29] e Izal [21] apresentam a observação do comportamento do protocolo na disponibilização de conteúdo no período de alguns meses. Qiu [30] utiliza um modelo de fluxos que representa o comportamento do protocolo para avaliar sua escalabilidade e desempenho no compartilhamento de arquivos. Bharambe [6] utiliza simulações para avaliar o comportamento do *BitTorrent* considerando métricas como utilização da banda pelos nós, tempo de *download* de arquivos e justiça entre os pares, utilizando variadas cargas de trabalho. Jun [23] avalia o mecanismo de incentivos do *BitTorrent* utilizando um modelo baseado em teoria dos jogos. Andrade [3] avalia o impacto das comunidades de compartilhamento de arquivos no desempenho do *BitTorrent*. Arthur [4] avalia a forma de disseminação de dados no *BitTorrent*. Feldman [20] apresenta uma visão geral sobre oportunismo em redes P2P (incluindo *BitTorrent*). É consenso entre esses trabalhos que, apesar do *BitTorrent* apresentar boa utilização da banda e velocidade no compartilhamento de arquivos, ele não possui um mecanismo de incentivos adequado e permite um certo nível de oportunismo e injustiça.

1.3 Organização do trabalho

Este trabalho está organizado da seguinte maneira: o capítulo 3 tratará do ataque Sybil e trará um estudo do comportamento do modelo original proposto por Rocha sob esse tipo de ataque, além de apresentar alterações aplicadas a esse modelo para melhor combater o ataque Sybil. O capítulo 4 apresentará o protocolo de rumores e apresentará também um estudo de como a aplicação desse protocolo afeta o comportamento do modelo de Rocha. Já o capítulo 5 detalha o comportamento do protocolo BitTorrent e apresenta a aplicação do modelo de reputações nessa rede. Dados experimentais para ilustrar cada alteração ao modelo de Rocha serão apresentados dentro de seus respectivos capítulos. Finalmente, o capítulo 6 trará as conclusões obtidas através desse trabalho, além da avaliação de possíveis trabalhos futuros.

Os gráficos apresentados neste trabalho não apresentam o desvio padrão das curvas para permitir maior legibilidade dos mesmos. Aqueles mais relevantes serão reapresentados com o desvio padrão em um apêndice.

Capítulo 2

Modelo original

Este capítulo apresenta em detalhes o comportamento do modelo baseado em reputação proposto por Rocha [33, 32] no ambiente de redes de roteamento sobrepostas. Alguns dados experimentais também são apresentados para demonstrar o comportamento desse modelo.

Uma rede de roteamento sobreposta é uma rede em nível de aplicação sobre o substrato de roteamento da Internet. Os nós membros monitoram o funcionamento e qualidade dos caminhos entre eles e usam esta informação para decidir por onde enviar seus pacotes com maior ganho segundo alguma métrica escolhida, como latência ou banda disponível [2].

Um princípio básico das redes de roteamento sobrepostas é que cada membro da rede deve contribuir com seus próprios recursos para poder utilizar aqueles disponibilizados pela rede. Se um participante da rede se recusar a prover serviço aos outros (comportamento chamado de *oportunista*), ele deveria ter suas requisições de serviço negadas pela rede, de modo a forçá-lo a ter um comportamento correto.

O modelo de Rocha utiliza um sistema de reputação para identificar e negar serviço a nós oportunistas, e ao mesmo tempo não interferir no serviço fornecido a nós de comportamento justo. Para isso, o modelo utiliza a reputação de um nó para avaliar se ele merece receber serviço e se ele é confiável para rotear mensagens de outros participantes da rede. Esse modelo será apresentado a seguir.

2.1 Descrição do modelo

Para poder operar, o modelo mantém um registro das requisições de roteamento feitas por cada nó a todos os demais, bem como dos resultados dessas requisições — isto é, se os outros nós as atenderam a contento. Com base nesse registro é possível obter a cada instante um balanço das interações entre dois nós i e j. Representamos por $S^t_{i(j)}$ o

saldo que i tem em relação a j em um dado instante t. Um nó i tem um saldo positivo na interação com um nó j se i forneceu mais serviço (banda) a j do que recebeu dele (ou seja, $S^t_{i(j)} > S^t_{j(i)}$).

A reputação de j segundo i ($R^t_{i(j)}$) representa quão vantajoso i acredita que uma transação com j será. Para calcular essa reputação, o modelo utiliza duas métricas que tem por objetivo representar a *experiência individual* de um nó com os demais e a *reputação* dos nós da rede reportada a um nó pelos demais. Essas métricas são construídas com base na relação entre as interações entre nós e os saldos entre eles.

Cada nó i possui um valor mínimo de reputação ($R_{min(i)}$), e para que ele aceite uma requisição de um nó j é necessário que $R^t_{i(j)} \geq R_{min(i)}$.

2.1.1 Experiência individual

A experiência individual $I^t_{i(j)}$ é definida como a visão particular que um nó i tem a respeito de um outro nó j, baseada apenas nas interações passadas entre eles. Toda vez que i tenta utilizar serviços de j, ele atualiza o valor da experiência individual com j de acordo com o resultado da interação. Caso j deva serviços a i, i considerará j injusto caso ele não atenda um pedido seu, o que será registrado na experiência individual $I^t_{i(j)}$.

Por outro lado, se o saldo de i em relação a j for nulo ou negativo (i não prestou mais serviços a j do que recebeu dele) j não tem qualquer obrigação de honrar pedidos de i, fazendo-o se assim preferir. Ou seja, um nó i não é considerado injusto ao negar serviço a um nó j se i forneceu mais serviço a j do que ele lhe forneceu em um determinado intervalo de tempo.

Sabendo reconhecer quando um nó foi injusto no fornecimento de serviço, é possível calcular a experiência individual ao se realizar uma transação. Para isso devemos considerar a quantidade de recursos solicitados por i (representada por r) e a quantidade de recursos provida realmente por j (representado por p). Dessa forma, $I^t_{i(j)}$ é representada pela Equação 2.1, onde podemos ver que há um incremento caso o pedido seja plenamente atendido ($p = r$) e uma redução caso contrário.

$$I^t_{i(j)} = \begin{cases} min(I^{t-1}_{i(j)} + \alpha, 1) & se\ p = r \\ \\ max(I^{t-1}_{i(j)} - (1 - \frac{p}{r})\alpha n^2, 0) & se\ S_{i(j)} - S_{j(i)} > 0\ e\ p \neq r \end{cases} \tag{2.1}$$

O α apresentado na equação é um parâmetro do modelo que indica o valor mínimo que a experiência individual cresce ou diminui a cada interação entre as partes. Já o n representa a quantidade de vezes que j já negou serviço completamente para i. Dessa forma o decréscimo de $I^t_{i(j)}$ será cada vez maior se j negar continuamente serviço a i.

É possível observar que a experiência individual diminui mais rapidamente do que aumenta. Isso é importante pois incentiva um participante a não parar de prover serviço depois de alcançar um valor alto de I. Ainda assim, permite que um nó que por algum motivo não conseguiu responder a todas as requisições recebidas ainda consiga melhorar sua reputação agindo com justiça.

Outro ponto importante é que um nó que consiga atender pelo menos parcialmente a uma requisição é menos penalizado do que um que negou serviço completamente, pois é mais provável que um nó que falhou apenas parcialmente tenha sofrido algum falha do que ele seja um oportunista.

Inicialmente a experiência individual de um nó com todos os outros da rede é igual a 0,5. Dessa forma, todos os nós consideram os demais confiáveis a princípio. Isso ocorre para não penalizar nós recém-chegados à rede.

2.1.2 Reputação reportada por outros nós (depoimentos)

Os depoimentos que um nó i coleta sobre um outro nó j ($T^t_{i(j)}$) representam a opinião de todos os outros participantes da rede a respeito de j e esse valor é calculado segundo a Equação 2.2.

$$T^t_{i(j)} = \frac{\sum_{k \in N} I^t_{k(j)} R^t_{i(k)}}{\sum_{k \in N} R^t_{i(k)}} \tag{2.2}$$

O valor do depoimento considera a experiência pessoal que todos os outros nós da rede tiveram com j, $I^t_{k(j)}$, e esse valor é ponderado pela reputação que i tem de cada um desses nós ($R^t_{i(k)}$). Isso torna necessário que i tenha conhecimento global das experiências pessoais de cada nó k com todos os outros nós da rede.

2.1.3 Reputação computada

O valor de reputação de j calculado por i ($R^t_{i(j)}$) indica o quanto i confia em j. A Equação 2.3 mostra como esse cálculo combina a experiência pessoal e os depoimentos recebidos.

$$R^t_{i(j)} = R^{t-1}_{i(j)} + \beta_i (T^t_{i(j)} - T^{t-1}_{i(j)}) + (1 - \beta_i)(I^t_{i(j)} - I^{t-1}_{i(j)}) \tag{2.3}$$

O valor da reputação computada é dependente do próprio valor de reputação anterior ($R^{t-1}_{i(j)}$), dos depoimentos que i possui de j ($T^t_{i(j)}$) e da experiência pessoal entre eles ($I^t_{i(j)}$). O parâmetro β, que varia entre 0 e 1, serve para definir o valor que os nós atribuem à opinião dos outros nós e à sua própria experiência pessoal, ou seja, um

valor maior de β significa que o nó i dará mais valor aos depoimentos sobre j do que à sua experiência pessoal com j.

2.2 O modelo original em funcionamento

Realizamos algumas simulações do modelo variando alguns de seus parâmetros para avaliar seu comportamento além do que foi reportado no artigo original. Esses experimentos consideraram uma rede com 110 nós, sendo 10 deles oportunistas, e foram simulados 50 vezes para obter dados mais homogêneos. Essas configurações, bem como a construção da rede simulada, seguem o trabalho original.

Inicialmente nossos experimentos utilizam a premissa dos nós oportunistas terem latência menor do que os nós justos, apresentada no trabalho original. Tendo os nós oportunistas menor latência, eles serão mais procurados para rotear pacotes, representando o pior caso da rede de roteamento, pois os nós oportunistas não rotearão as mensagens recebidas, causando particionamento na rede e diminuindo a sua confiabilidade. Além disso, o valor de proporção de requisições aceitas apresentado é referente à *possibilidade* de um nó justo aceitar uma requisição de um nó oportunista (dada pelo valor de reputação atual do oportunista e pelo valor de reputação mínima de cada nó justo), e não resultado de requisições aceitas de fato.

2.2.1 Parâmetros básicos do modelo

O primeiro parâmetro a ser observado é o α, que identifica quanto a experiência individual varia a cada interação. Como podemos verificar na Figura 2.1, valores maiores de α fazem com que os nós oportunistas sejam identificados e punidos mais rapidamente, ainda que por uma margem pequena. Isso se dá pelo fato da reputação dos oportunistas chegar a valores mais baixos com menos interações.

O segundo parâmetro observado é β, que indica o quanto um nó confia na sua experiência individual e o quanto ele confia no testemunho dos outros nós. Quanto maior o valor de β, mais um nó valoriza os testemunhos e menos sua experiência individual. O comportamento do modelo com valores de β variados pode ser observado na Figura 2.2.

Pode-se verificar que quanto maior o valor de β, mais rápido os nós justos identificam os nós oportunistas. Isso se dá porque eles terão mais informações em que basear sua opinião sobre um dado nó. Em muitos casos, nós serão capazes de identificar um nó oportunista antes mesmo de ter qualquer interação direta com o mesmo, evitando o desperdício de recursos que haveria nesse caso.

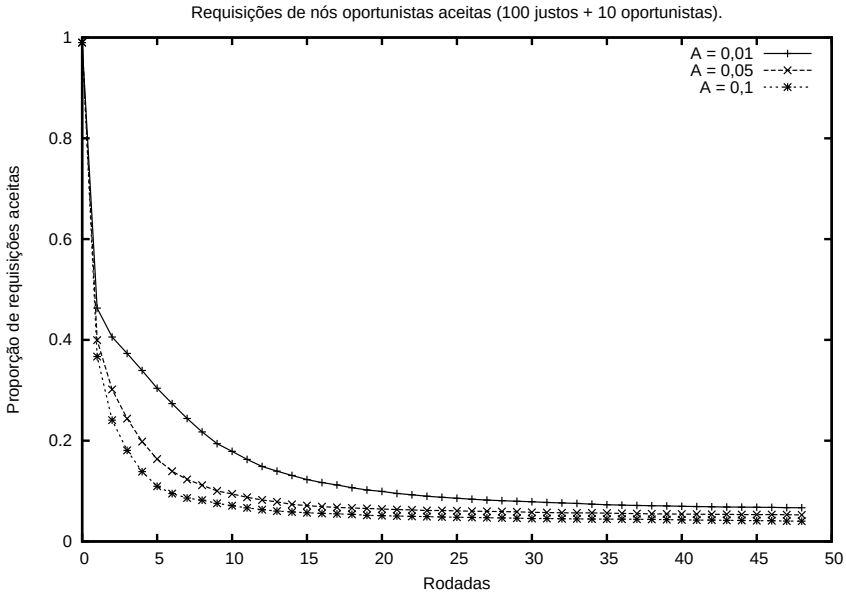


Figura 2.1: Variação de α

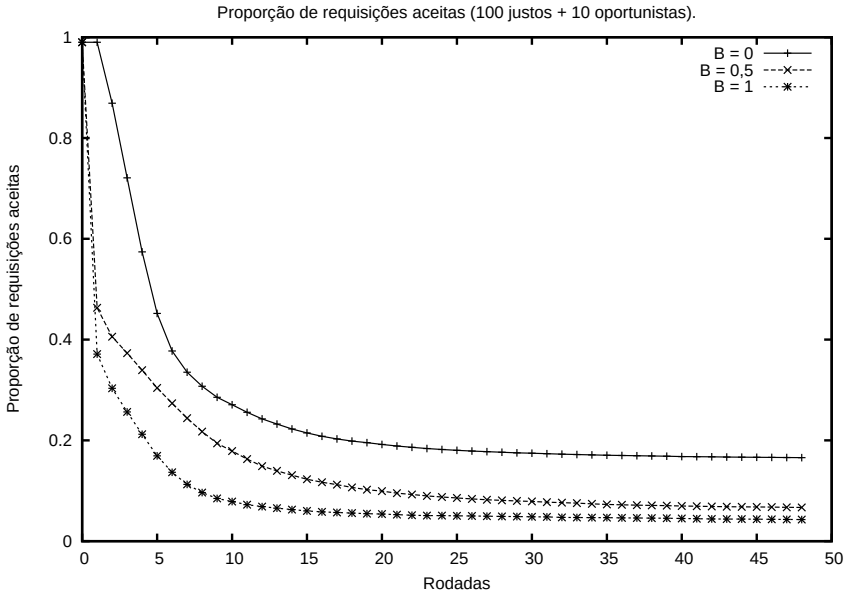


Figura 2.2: Variação de β

Considerando esses resultados, utilizaremos, por simplicidade, $\alpha = 0,01$ no restante dos experimentos apresentados neste trabalho (exceto quando explicitado o contrário), visto que a diferença causada pelo aumento deste parâmetro não causa grande ganho no desempenho do sistema.

2.2.2 Recuperação de um nó

Um elemento importante do sistema de reputações é que um nó que por algum motivo não responda a algumas requisições (e portanto seja penalizado com a diminuição de sua reputação) ainda é capaz de recuperar seu status de justo ao passar a responder a todas as requisições recebidas.

Um fator muito importante para a recuperação de um nó da rede é o valor da reputação mínima (R_{min}). Temos que $0 < R_{min} \leq 0,5$, com os valores de R_{min} sendo assinalados da seguinte forma: um valor aleatório e uniformemente distribuído entre 0 e 1 é gerado, caso esse valor seja menor que $0,5$, esse valor será mantido como reputação mínima, caso contrário a reputação mínima será igual a $0,5$. Essa distribuição é usada para garantir que existam alguns nós mais "tolerantes", importantes para dar a chance a nós de baixa reputação que desejem se redimir. Esses nós começariam a recompor sua reputação à medida que interagirem positivamente com nós mais tolerantes.

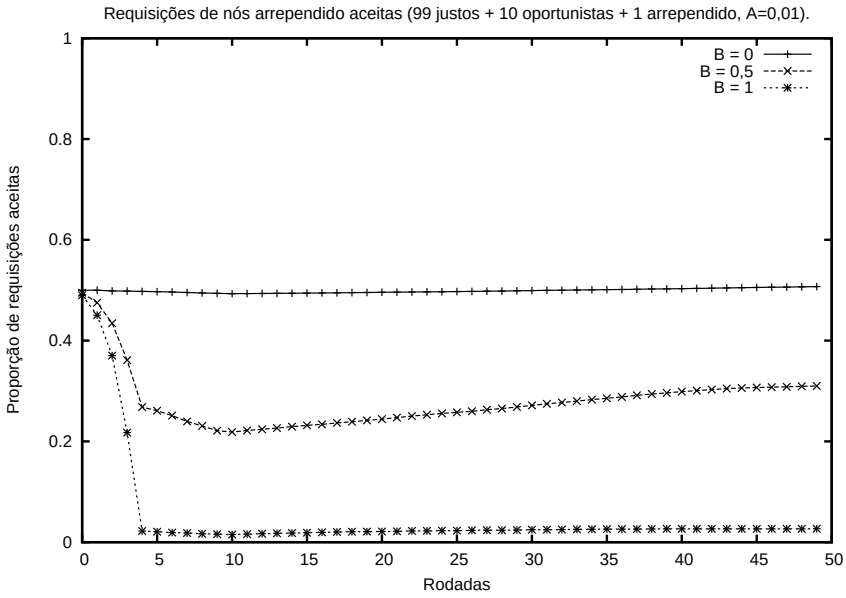


Figura 2.3: Reputação de um nó arrependido com variação de β

A Figura 2.3 apresenta a proporção de serviço recebido por um nó que inicialmente age como oportunista e depois da rodada 10 passa a agir de forma justa. Para valores de β mais baixos, tanto a queda quanto o aumento da reputação são muito pequenos (a curva com $\beta = 0$ mal parece ser alterada, apesar de haver queda e aumento dela), devido ao uso apenas de experiência individual para calcular a reputação. Para $\beta = 0,5$ podemos verificar uma queda mais visível, além do incremento também mais significativo após a mudança de comportamento do nó. Já a curva de $\beta = 1$ apresenta uma queda muito acentuada (como previsto para esse valor) e um aumento muito pequeno

de reputação após a mudança de comportamento. Isso ocorre pois poucos nós (de baixa reputação mínima) rotearão mensagens através do nó arrependido, o que causará um aumento bastante lento da sua reputação.

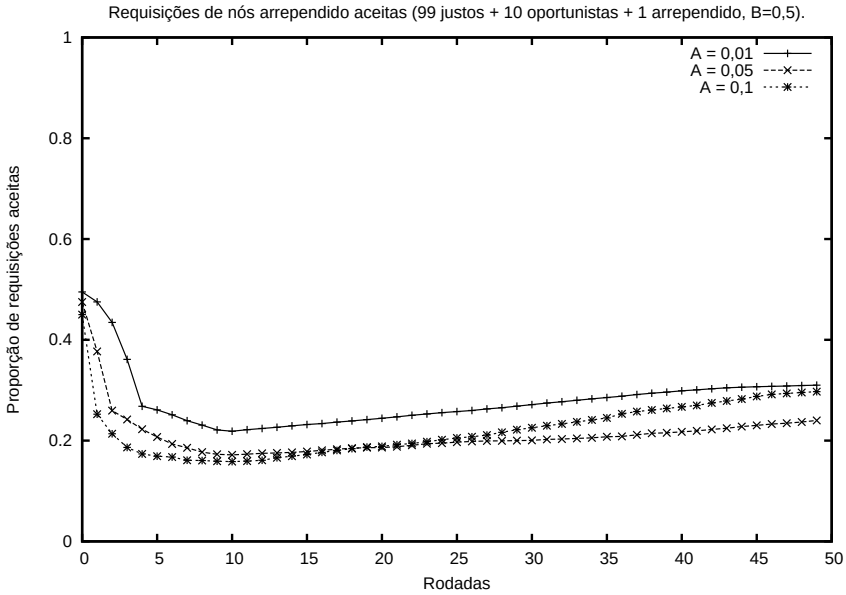


Figura 2.4: Reputação de um nó arrependido com variação de α

Já a Figura 2.4 apresenta a variação da reputação do nó arrependido. Podemos verificar que, quanto maior o valor α, mais rapidamente a curva decai e também cresce.

2.2.3 Nível de oportunismo aceito

A equação 2.1, apresentada anteriormente, mostra que a experiência individual decai mais rapidamente do que cresce, pois ao passo que o aumento é aditivo com base no parâmetro α, o decréscimo é dado pela subtração desse mesmo α multiplicado pelo quadrado do número de falhas sucessivas ocorridas com esse mesmo nó.

Como nós adquirem boa reputação ao atender pedidos, um nó malicioso pode tentar usar os serviços da rede atendendo apenas a uma fração dos pedidos que recebe. Esse comportamento, entretanto, é desestimulado pela forma como os pedidos não aceitos pesam mais que aqueles aceitos. O gráfico da Figura 2.5 apresenta a proporção de serviço recebido por nós oportunistas que recusem apenas uma fração das requisições recebidas. Podemos observar que aceitando até 80% das requisições recebidas um nó oportunista ainda consegue ter mais de 90% das suas requisições atendidas, mas qualquer negação maior que essa já causa uma queda maior no serviço recebido. Esse comportamento ocorre devido à própria forma que o decréscimo da experiência individual ocorre, pois ela diminui com maior intensidade apenas no caso de comporta-

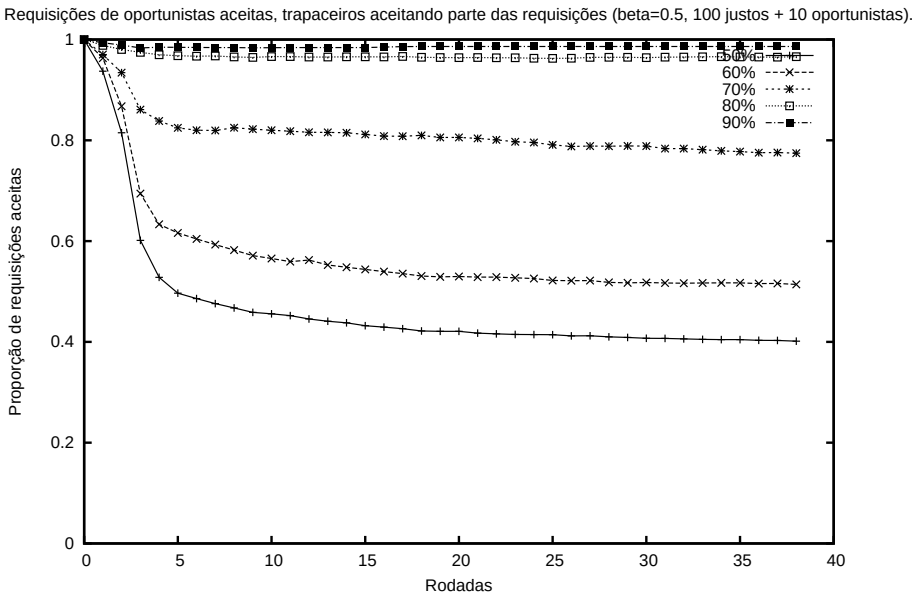


Figura 2.5: Serviço fornecido a oportunistas quando eles aceitam parte das requisições

mento injusto realizado contra um mesmo nó realizado seguidamente (dado pelo n^2 da equação 2.1). Ou seja, se a negação de serviço a um nó for intercalada por fornecimento de serviço a esse mesmo nó com uma probabilidade alta, o decréscimo da experiência individual será sempre pequeno.

Capítulo 3

O ataque Sybil

Redes sobrepostas e sistemas Par-a-Par utilizam a existência de múltiplas entidades independentes para diminuir a ameaça de elementos hostis, compartilhando recursos e impedindo que haja um ponto único de falha na rede. Para uma ação hostil ser significativa em um ambiente desse tipo seria necessário que a entidade maliciosa obtivesse o controle de uma parcela considerável dos nós dessa rede.

O ataque Sybil[1] foi discutido inicialmente por Douceur [18]. Ele consiste em uma única entidade utilizar várias identidades (forjadas ou roubadas) para acessar uma determinada rede. Dessa forma, uma entidade maliciosa pode utilizar um número arbitrário de identidades (dependente apenas de suas restrições físicas) e assim obter controle de uma fração considerável da rede. Uma vez possuindo um grande número de identidades virtuais sob seu controle, a entidade maliciosa pode usar essa "força através dos números" para inutilizar ou manipular sistemas como votação, armazenamento distribuído e roteamento.

Por exemplo, em um sistema de votação uma entidade maliciosa com várias identidades virtuais (que são conhecidas como identidades Sybil) pode utilizá-las para sempre apoiar o resultado que ela deseje que seja vitorioso na votação. Com uma quantidade grande o suficiente de Sybils ela poderia ditar o resultado de toda e qualquer votação. Um sistema de armazenamento distribuído que utilize a divisão de um arquivo entre vários participantes para garantir a segurança e privacidade desse arquivo pode acabar fornecendo as diferentes partes do arquivo para identidades Sybil sob o comando de uma mesma entidade maliciosa. Em uma rede de roteamento, se as identidades Sybil apresentarem menor latência entre si e estiverem dispersas pela rede, a entidade maliciosa pode se tornar responsável por boa parte das rotas utilizadas, podendo então realizar outros ataques como *buraco negro* (onde os nós não retransmitem nenhuma

[1] Batizado com o nome da personagem principal do livro [36] e filme [28] homônimos, que relatam um caso famoso de distúrbio de personalidade múltipla nos EUA.

mensagem para os destinatários) ou *retransmissão seletiva* (onde apenas uma fração das mensagens são retransmitidas para seus destinatários).

Sendo uma identidade virtual apenas uma abstração utilizada no acesso a uma rede ou sistema, existe uma grande dificuldade em identificar identidades virtuais apresentadas por uma mesma entidade real. Uma forma de fazer isso é utilizar uma entidade centralizada confiável que possa certificar cada usuário, seja através de uma autoridade explícita como no sistema Farsite [1], ou através de uma autoridade implícita como no sistema CFS [13]. Porém, quando o uso de uma entidade centralizada confiável não é possível (como em redes P2P de compartilhamento de arquivos), esse tipo de identificação ainda é um problema em aberto.

3.1 Comportamento do modelo original diante de um ataque Sybil

O modelo original de Rocha considera que os nós oportunistas são entidades independentes e egoístas, buscando lucro apenas para si próprios. Todavia, se considerarmos que os nós oportunistas são apenas representações de uma mesma entidade real, eles podem agir em conluio para subverter o sistema de reputações. Por exemplo, se todos os nós em conluio reportarem para a rede que tiveram experiências positivas uns com os outros, ao mesmo tempo que agem de forma oportunista com o resto da rede, o sistema de reputação não refletirá a realidade, pois as duas opiniões (que os nós em conluio são justos e que eles são oportunistas) terão ambas um bom número de defensores. Um ataque Sybil facilita a ocorrência desse tipo de situação, pois torna-se necessária apenas uma entidade real para criar um conjunto grande de identidades virtuais que trabalharão em conluio.

O Figura 3.1 mostra o comportamento do modelo diante de um ataque Sybil conforme descrito acima, em uma rede com 100 nós justos, 10 nós Sybil e $\alpha = 0,05$ (onde α indica a quantidade mínima que o valor de experiência individual aumenta ou diminui a cada interação entre dois nós). Podemos observar que à medida que os nós Sybil alimentam a rede com informações adulteradas sobre seu comportamento, eles passam a ser mais confiáveis aos olhos dos outros participantes. Esse comportamento só não ocorre no caso de $\beta = 0$, pois nesse caso os nós não utilizam a opinião de outros nós para o cálculo da reputação. Entretanto, como mostrado no trabalho de Rocha [32], o uso de $\beta > 0$ é vantajoso em outros casos. Essas curvas possuem um desvio padrão médio menor que $0,13$, sendo que nos casos de $\beta \geq 0,5$ o desvio padrão médio aumenta com o passar das rodadas, o que indica a instabilidade do modelo quando exposto à contradição de informações sobre os nós Sybil..

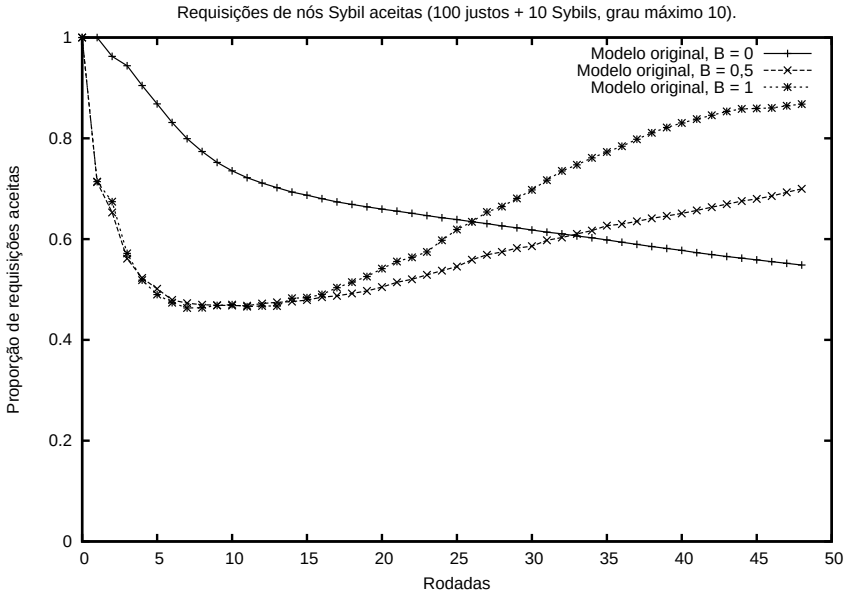


Figura 3.1: Requisições de nós Sybil aceitas no modelo original

Em uma variação desse ataque, além de reportarem justiça entre si, os nós Sybil também podem *difamar* um nó justo reportando para o resto da rede que o nó difamado agiu de forma oportunista para com eles, de modo que ele passe a ser considerado um oportunista pelos outros nós da rede, apesar de não sê-lo, e acabe sendo excluído da rede, como visto na Figura 3.2. O gráfico nos mostra que a difamação diminui drasticamente a quantidade de serviço obtido pelo nó difamado, mas considerando que a experiência individual reportada pelos Sybils sobre o nó difamado não podem ser menores que 0, uma vez que eles cheguem ao ponto de reportarem esse valor o nó difamado pode iniciar um processo similar a o de um nó arrependido, oferecendo serviço para nós com reputação mínima baixa para poder aumentar sua própria reputação. No entanto, se um número maior de nós Sybil for utilizado o nó difamado pode ser completamente excluído da rede antes de ter a oportunidade de se "redimir". O desvio padrão médio dessa curva chega ao máximo de $0,15$ no fim da curva, e apresenta a mesma característica de aumentar suavemente com o número de rodadas de simulação [2].

É interessante notar que esse tipo de ataque é de grande interesse hoje, e foi mesmo mencionado em um comentário de um leitor sobre o artigo original de Rocha [32], publicado em uma edição posterior da mesma revista[3].

[2] Os gráficos com barras de desvio padrão serão apresentados no Apêndice.

[3] "Letters to the Editor", IEEE Internet Computing, julho - agosto de 2006, pg 10, v. 10, n. 4

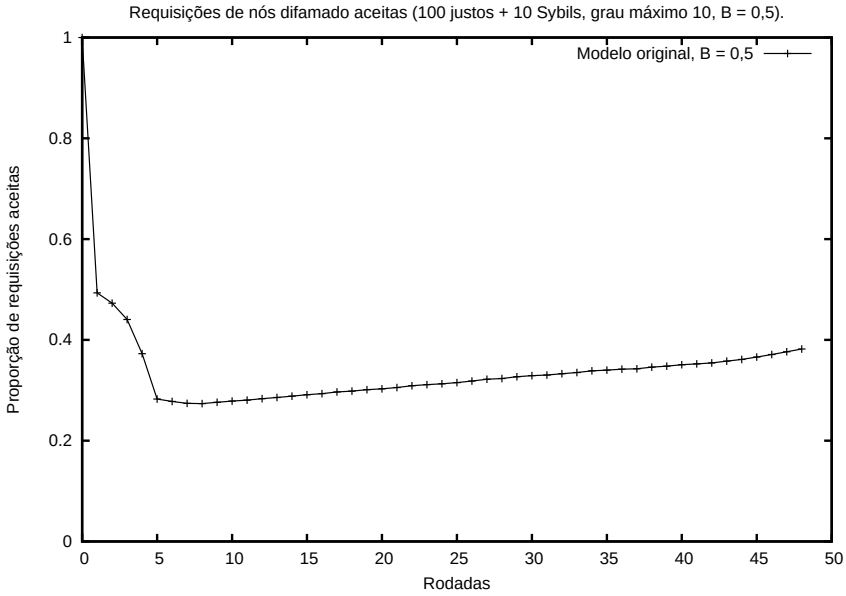


Figura 3.2: Requisições de um nó justo aceitas quando nós Sybil em conluio tentam difamá-lo

3.2 Alterações no modelo original para lidar com o ataque Sybil

Considerando esse novo ambiente onde o conluio entre nós maliciosos pode ocorrer, a reputação calculada pode não representar aquilo que realmente ocorre na rede e, portanto, precisa ser revista.

Inicialmente é importante relembrar como a reputação é calculada no modelo original para entendermos as limitações nesse caso. A Equação 3.1 repete o cálculo da reputação no modelo original. Podemos observar que a ponderação entre o peso dado à experiência individual ($I^t_{i(j)}$) com o nó avaliado e a opinião geral dos outros nós da rede sobre o nó avaliado (representado pelo testemunho dos pares $T^t_{i(j)}$) é feita pelo parâmetro β. Porém, como visto na Figura 3.1, apenas a variação de β não nos dá resultados melhores. Dessa forma, precisamos identificar como o conluio dos nós Sybil pode ser melhor identificado.

$$R^t_{i(j)} = R^{t-1}_{i(j)} + \beta_i(T^t_{i(j)} - T^{t-1}_{i(j)}) + (1 - \beta_i)(I^t_{i(j)} - I^{t-1}_{i(j)}) \tag{3.1}$$

Mudemos então o foco para o testemunho dos pares, sendo esse valor definido no modelo original segundo a Equação 3.2. Podemos ver que o testemunho é calculado usando a experiência pessoal que cada nó k da rede tem com o nó alvo j, ponderado pela reputação que o nó i, que calcula a métrica, tem de k. Dessa forma, quando i

tenta calcular o testemunho de um nó Sybil, as experiências individuais altas relatadas pelos outros nós Sybil fará com que o valor do testemunho fique alto.

$$T_{i(j)}^{t} = \frac{\sum_{k \in N} I_{k(j)}^{t} R_{i(k)}^{t}}{\sum_{k \in N} R_{i(k)}^{t}} \tag{3.2}$$

No modelo original, a idéia de se ponderar os relatos de k pela sua reputação como observada por i tinha por objetivo reduzir o impacto de relatos vindos de nós de baixa reputação. Entretanto, está claro que essa solução falha no caso de vários nós em conluio, pois mesmo reduzidos individualmente, o efeito acumulativo ainda é significativo, o que leva à elevação gradual das curvas para $\beta \neq 0$ na Figura 3.1.

Considerando isso, defendemos que seja o uso indiscriminado (mesmo ponderado) de opiniões de outros nós que permite que a influência dos nós Sybil torne-se danosa ao sistema de reputações. Portanto, acreditamos que deva haver uma maior restrição sobre quais nós podem ser considerados confiáveis no momento do cálculo do testemunho dos pares. Nós propomos duas políticas para identificar nós que sejam confiáveis para ter suas opiniões consideradas: confiança baseada na experiência pessoal e confiança baseada na reputação computada, que serão analisados a seguir.

3.2.1 Confiança baseada na experiência individual

Aqui consideramos que um nó i confia na informação provida por um nó j se $I_{i(j)}^{t} > 0,5$. Ou seja, i só utilizará as informações de experiência individual de um nó j para o cálculo de testemunhos se o valor da experiência individual de i com j for maior que 0,5. Considerando que todos os nós iniciam com experiência individual *igual* a 0,5, inicialmente nenhuma informação de experiência individual de outros nós será utilizada no cálculo de reputação. A informação obtida com um outros nó j só será utilizada no cálculo de reputações após ocorrer pelo menos uma transação positiva com ele.

Isso altera a fórmula para cálculo dos depoimentos que i recebe sobre j para aquela apresentada na Equação 3.3.

$$T_{i(j)}^{t} = \frac{\sum_{k} I_{k(j)}^{t} R_{i(k)}^{t}}{\sum_{k} R_{i(k)}^{t}} \ , \ k \in N | I_{i(k)}^{t} > 0,5 \tag{3.3}$$

O uso ponderado pela reputação dos nós ainda é mantido para manter o princípio do modelo original, valorizando mais o depoimento de nós mais confiáveis.

3.2.2 Confiança baseada em reputação

Nesse caso, consideramos que um nó i confia em um nó j se $R^t_{i(j)} > 0,5$. Isso significa que um nó i somente aceita informações de experiência individual de um nó j se a reputação que i conhecer de j for maior que 0,5. Da mesma forma que acontece no caso da confiança, como a reputação calculada a princípio é igual a 0,5, os nós não aceitarão informações dadas por todos os nós no cálculo do testemunho. A diferença para a confiança baseada em experiência individual é que nesse caso é possível passar a confiar em um outro nó j sem ter necessariamente que realizar uma transação direta com ele, pois a reputação que i conhece de j pode aumentar se a experiência pessoal de um outro nó k com j for alta e i confiar em j.

A nova fórmula para o cálculo dos depoimentos é dada pela Equação 3.4.

$$T^t_{i(j)} = \frac{\sum_k I^t_{k(j)} R^t_{i(k)}}{\sum_k R^t_{i(k)}} \ , \ k \in N | R^t_{i(k)} > 0,5 \tag{3.4}$$

Novamente a ponderação desse fator pela reputação é mantida.

3.3 Comparação entre os modelos

Realizamos alguns experimentos para comparar o comportamento dessas duas alterações com o modelo original. Esses experimentos utilizaram redes com 100 nós justos e 10 nós Sybil, sendo que os nós Sybil publicam informação afirmando que tiveram sucesso em transações uns com os outros a cada rodada. Utilizamos $\alpha = 0,01$ em todas as simulações Também restringimos o grau dos nós participantes da rede para no máximo 10. Os modelos são aplicados a uma aplicação de roteamento sobreposto.

Além de avaliar o comportamento com nós Sybil, as comparações incluem também o impacto sobre nós justos e oportunistas, para avaliar o efeito sobre as premissas originais.

3.3.1 Serviço fornecido a nós Sybil

A Figura 3.3 apresenta o comportamento dos 3 modelos (original, confiança baseada na experiência individual e confiança baseada na reputação computada) quando $\beta = 0$. Podemos notar que, como com $\beta = 0$ a experiência individual é a única métrica levada em consideração no cálculo da reputação, todos os modelos apresentam o mesmo comportamento, uma vez que as alterações propostas alteram o uso de informação de testemunhos de outros nós. O desvio padrão médio dessa curva não ultrapassa $0,6$ para toda a curva.

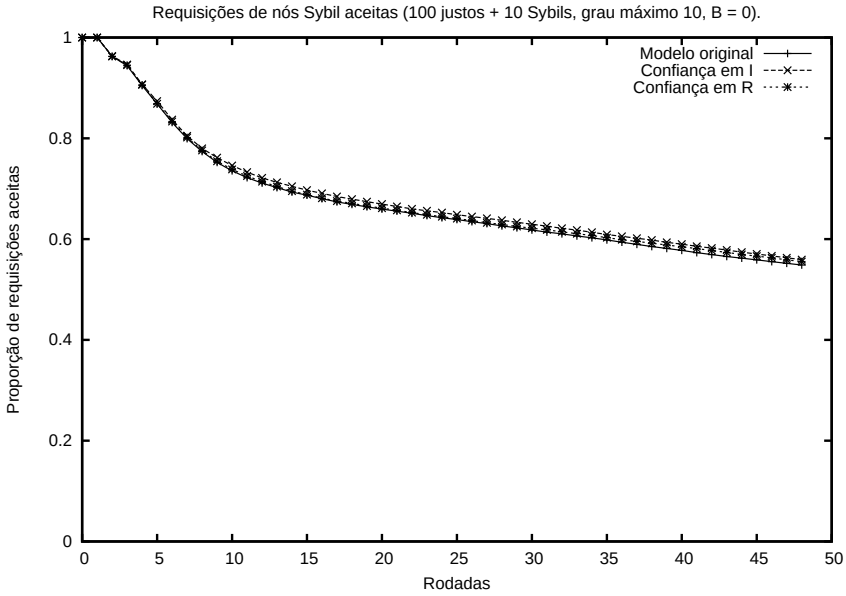


Figura 3.3: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0$

Já a Figura 3.4 apresenta a comparação dos modelos quando $\beta = 0,5$. Podemos observar que o modelo original começa a aceitar novamente requisições de nós Sybil depois de um certo tempo, devido ao comportamento dos Sybils de publicar informação positiva uns sobre os outros a cada rodada. Já os modelos alterados não apresentam essa tendência a voltar a aceitar requisições de Sybils, pois uma vez que eles os considerem oportunistas eles não mais usarão suas opiniões para o cálculo da reputação de outros nós, dessa forma eliminando a influência de seus testemunhos adulterados. O desvio padrão médio das curvas referentes às aletações não ultrapassa $0,5$ durante todo o experimento.

Podemos notar também que o modelo que usa confiança baseada em reputação apresenta um desempenho um pouco melhor que o de confiança baseada em experiência individual. Isso ocorre porque o modelo baseado em reputação pode passar a confiar nas opiniões de outros nós justos mesmo sem ter experiências diretamente com eles, o que não ocorre no modelo baseado em experiência individual. Com mais informações fornecidas por nós justos, mais fácil se torna o processo de descoberta de nós Sybil.

A Figura 3.5 apresenta a mesma comparação dos anteriores, mas com $\beta = 1$. Podemos notar que o comportamento de voltar a aceitar requisições de nós Sybil persiste no modelo original de forma mais aguda, pois com $\beta = 1$ dá-se maior valor aos depoimentos de outros nós (incluindo Sybils). Os modelos alterados também apresentam comportamento similar ao caso com $\beta = 0,5$, porém conseguem, ao fim da simulação, excluir mais de requisições de nós Sybil, mesmo que por uma margem pequena. Assim

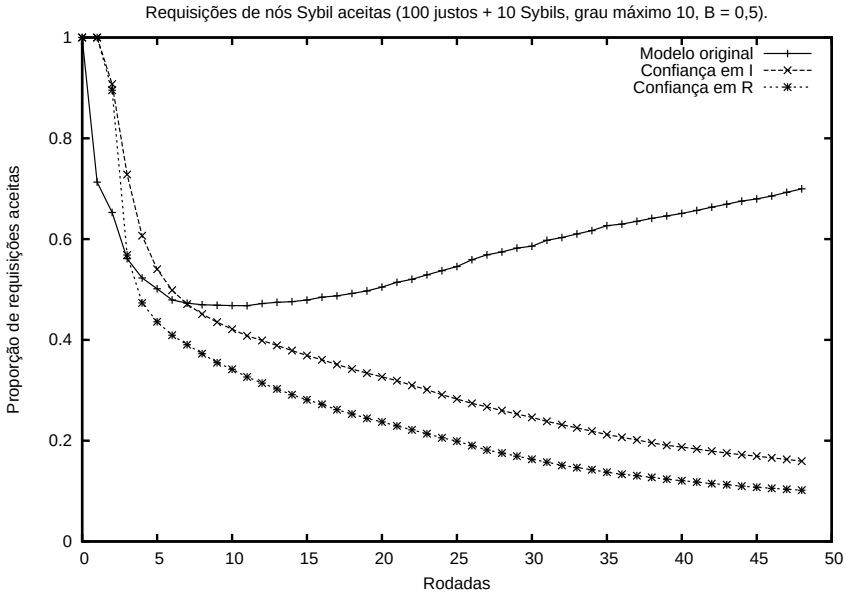


Figura 3.4: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$

como para $\beta = 0,5$, o desvio padrão médio das curvas alteradas não ultrapassa $0,5$.

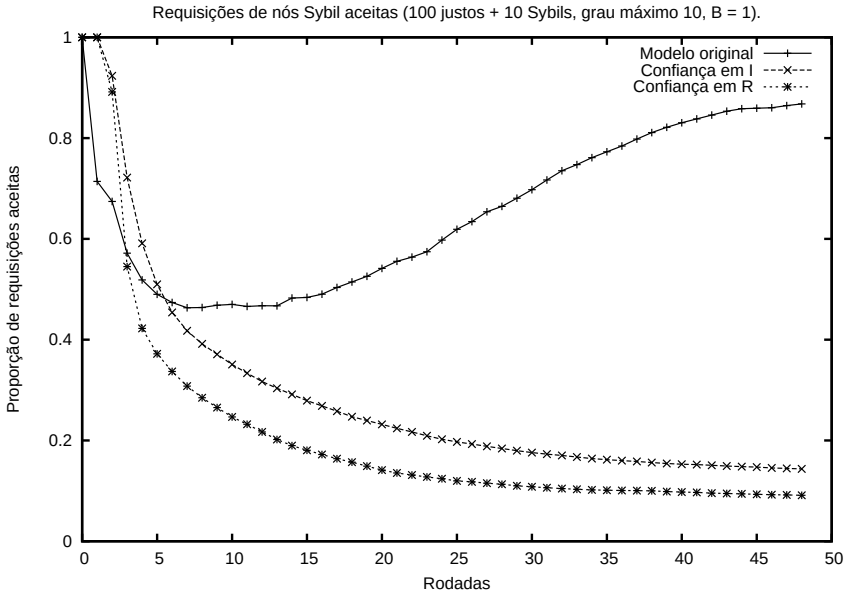


Figura 3.5: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 1$

3.3.1.1 Difamação com nós Sybil

Como vimos anteriormente nesse capítulo, é possível que os nós Sybil agindo em conluio além de reportarem experiências positivas entre si podem também reportar em conjunto que um nó justo apresenta comportamento oportunista, mesmo sem que ele o seja, num processo de difamação. A Figura 3.6 apresenta o comportamento do modelo original e dos modelos alterados quando um nó sofre difamação de um conjunto de nós Sybil. Podemos observar que, no modelo original, os nós Sybil conseguem difamar o nó justo até um determinado ponto onde mesmo com suas reputações altas eles não conseguem mais fazer sua opinião subjugar a opinião do restante da rede, de forma que a partir desse ponto o nó difamado passa a ser "redimido" pelos outros nós justos. Já os modelos alterados, como não utilizam as informações de outros nós até validá-los com o valor de experiência individual ou de reputação que eles conhecem deles, as opiniões dos nós Sybil não causarão alteração na opinião que eles possuem sore o nó difamado, de forma que o serviço fornecido a eles não sofre queda.

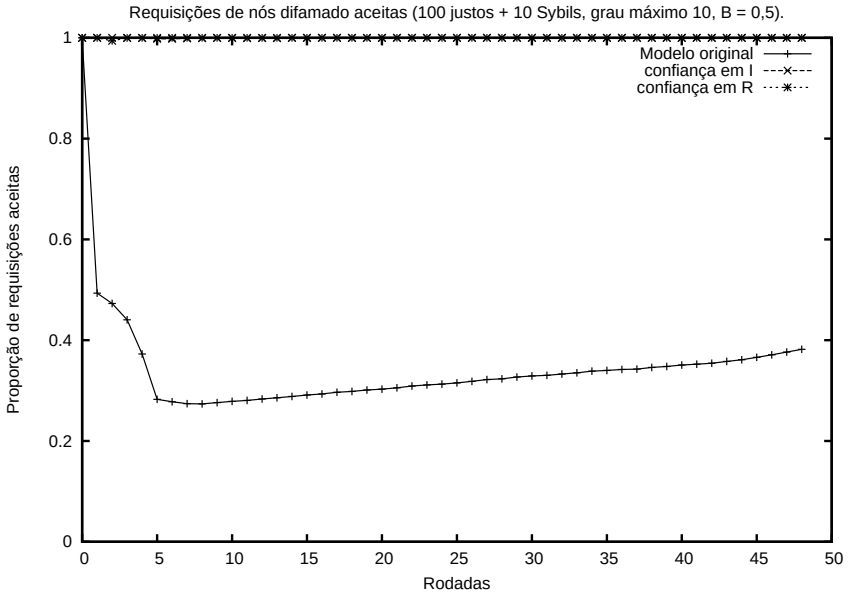


Figura 3.6: Requisições de um nó difamado por Sybils aceitas nos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$

3.3.2 Serviço fornecido a nós justos

É importante que as alterações não diminuam a qualidade do serviço fornecido a nós justos. Podemos observar na Figura 3.7 que todas as variações de β em cada modelo apresentam alto nível de serviço para nós justos, tendo diferenças inferiores a 1% entre si.

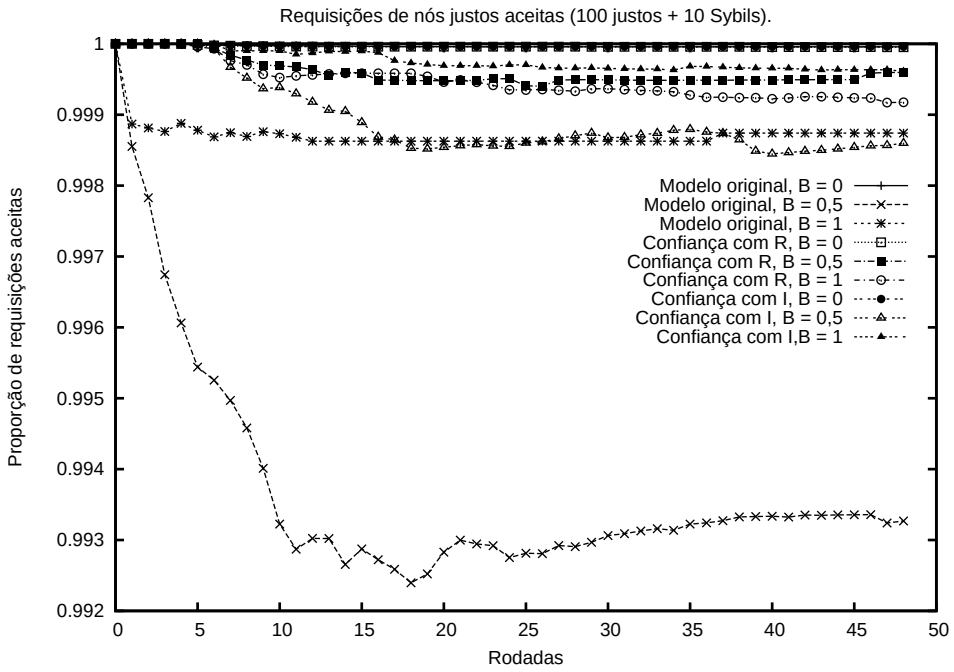


Figura 3.7: Requisições de nós justos aceitas

3.3.3 Serviço fornecido a nós oportunistas

Uma vez que estamos propondo uma mudança no modelo anterior, é importante verificar o impacto dessas mudanças na aplicação original do modelo. Podemos observar na Figura 3.8 que para $\beta = 0$ não há grande diferença no comportamento dos 3 modelos, pois em nenhum deles haverá o uso de informações de pares no cálculo da reputação.

Já na Figura 3.9, com $\beta = 0,5$ observamos que o modelo original apresenta um comportamento um pouco superior às duas alterações propostas, sendo que entre as alterações a que apresenta confiança baseada em reputação computada apresenta o desempenho mais próximo ao do modelo original. Isso se dá porque o modelo original possui muito mais informações para identificar nós maliciosos do que as alterações propostas, que limitam de forma proposital a quantidade de nós cuja opinião será considerada no momento do cálculo da reputação. No caso de nós que não trabalham em conluio até a opinião de nós oportunistas é interessante, pois se eles não receberem serviço de outro oportunista eles irão denunciá-lo à rede, coisa que não ocorre no caso de conluio. Também é possível verificar que as curvas dos modelos alterados demoram mais para iniciar a queda devido ao uso restrito de informações no início da simulação, quando nenhum nó considera o resto da rede confiável para o cálculo da reputação.

A Figura 3.10 apresenta a comparação para $\beta = 1$. Podemos observar que ao final da simulação todas as curvas alcançam um nível de exclusão de requisições de oportunistas mais alto do que no caso de $\beta = 0,5$, ainda que apresentando um comportamento

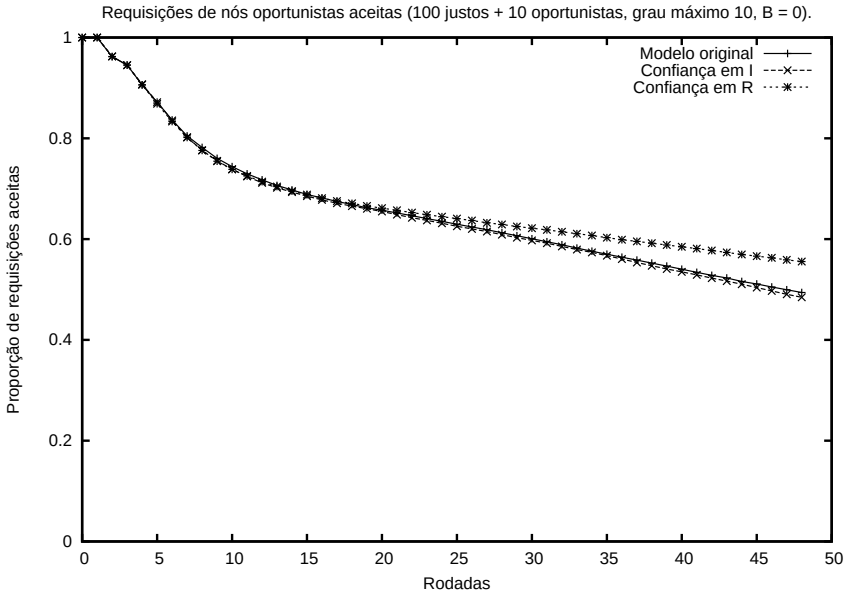


Figura 3.8: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0$

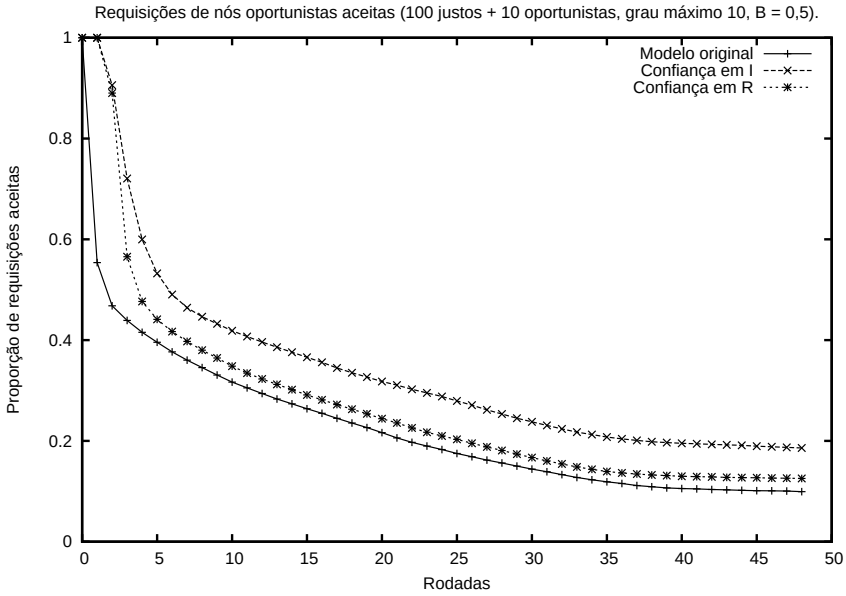


Figura 3.9: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$

bastante similar a ele.

O desvio padrão médio para todas as curvas e valores de β apresentados nesse caso não excede $0,5$.

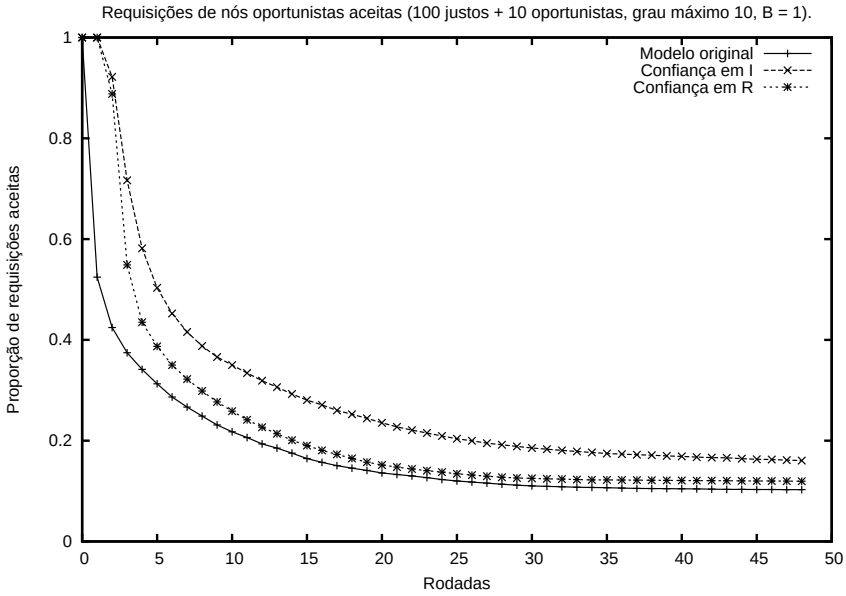


Figura 3.10: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 1$

3.4 Sumário

Observamos neste capítulo que o modelo original da forma que foi proposto não apresenta bom comportamento diante de nós oportunistas em conluio e propusemos algumas alterações no modelo para que ele pudesse combater esse tipo de situação. As alterações propostas conseguiram não só combater de forma mais eficiente o conluio entre oportunistas como também manteve o mesmo nível de serviço fornecido a nós justo que o modelo original fornece. Além disso, apesar do uso de menos informações para o cálculo da reputação, as alterações propostas conseguem resultados bem próximos aos alcançados pelo modelo original na exclusão de nós oportunistas, especialmente o modelo com confiança baseada na reputação computada.

Capítulo 4

Protocolo de rumores

No modelo original de Rocha [32, 33] o sistema pressupõe que existe um conhecimento global das opiniões que cada nó possui sobre todos os outros, e cada atualização é imediatamente visível para os outros membros da rede (o que requer $O(n^2)$ mensagens). Um conhecimento global dessa forma é uma restrição significativa, mas aceitável no contexto de redes de roteamento considerado naquele trabalho. Em um ambiente de redes P2P amplamente distribuídas, tal restrição torna-se mais difícil de ser atendida, pois diminuiria drasticamente a escalabilidade da rede.

Em ambientes distribuídos onde um estado global deve ser mantido e o mesmo pode ser atualizado de forma distribuída em diversos pontos da rede, mecanismos de disseminação direta de atualizações, onde cada atualização do estado global é informada de forma atômica a todos os participantes, podem causar congestionamento na rede, resultando na perda de mensagens e num estado inconsistente de informações ou em um excesso de sincronia entre os pares.

Dessa forma, para diminuir o *overhead* de mensagens para manutenção desse estado global, decidimos utilizar um protocolo de rumores para disseminar as informações de experiência individual entre os participantes da rede.

Uma saída para o problema de manutenção de estado global é o uso de algoritmos epidêmicos ou protocolos de rumores (*gossip*) [16, 15, 25, 34]. Nesses algoritmos, cada atualização é repassada a um vizinho por vez. Caso o receptor não tenha conhecimento dessa atualização, ele a efetua e a armazena como um "rumor quente". Um nó com um "rumor quente" tentará repassá-lo para seus vizinhos, que reagirão da mesma forma caso não o conheçam. Se um nó tentar mandar uma atualização para um nó que já a possua, ele poderá deixar de considerar a atualização como "rumor quente" (com uma determinada probabilidade ou com um contador de contatos desnecessários), momento no qual guardará o rumor, mas não tentará mais difundi-lo.

4.1 Funcionamento de um protocolo de rumores

Os nós em um protocolo de rumores podem apresentar três comportamentos em relação a um rumor:

- **Suscetível:** o nó não conhece o rumor e está apto a recebê-lo.
- **Infeccioso:** o nó conhece o rumor e tenta ativamente passá-lo para nós suscetíveis. Ou seja, ele possui um rumor quente.
- **Infectado:** o nó conhece o rumor, mas não tem mais interesse em repassá-lo para outros nós. Ou seja, ele possui um rumor frio.

Protocolos *gossip* podem trabalhar com dois comportamentos, *push* ("empurrar") ou *pull* ("puxar") . No caso *push* , um nó com um rumor quente tenta passar ativamente este rumor para outros nós. Já no caso *pull*, cada nó periodicamente pergunta a um vizinho se ele tem algum novo rumor. Essa periodicidade pode se dar com um contador, probabilidade ou ocorrência de algum evento. Estas variações existem para maximizar algum aspecto da disseminação de informação, como menor tempo de disseminação, menor probabilidade de nós ficarem sem atualização, menor *overhead* de comunicação, etc.

Quando apresenta o comportamento *push*, um nó infeccioso tenta periodicamente enviar sua nova atualização para um de seus vizinhos (escolhido de forma aleatória). Esse nó decidirá que sua atualização não é mais interessante com uma probabilidade $\frac{1}{k}$ (onde k é um parâmetro decidido pelo projetista) cada vez que ele tenta mandar uma atualização para um nó que já a conheça ou com um contador (ele tentará mandar a atualização para um número fixo de pares). Esse comportamento tem como vantagens ter um atraso menor na disseminação de uma atualização para toda a rede e utilizar menos mensagens para repassar uma atualização.

A Figura 4.1 apresenta o comportamento da rede na transmissão de uma atualização utilizando *push*. Inicialmente temos apenas o nó 1 infeccioso na figura 4.1(a), tentando passar a atualização para o nó 3. Em 4.1(b) o nó 3 tornou-se infeccioso e tenta passar a atualização para frente. Na Figura 4.1(c) o nó 1 tenta mandar uma atualização para um nó que já a conhece (no caso, 3), dessa forma ele passará a ficar apenas infectado em 4.1(d)(denotado pelo tom mais claro do nó), não mais tentando propagar a atualização. O processo segue na Figura 4.1(e) até terminar sem nenhum nó infeccioso (ou seja, ninguém mais tenta repassar a atualização) na Figura 4.1(f).

Podemos notar que na Figura 4.1(f) o nó 8 terminou sem ter conhecimento da atualização. Essa é a desvantagem do comportamento *push*. Existe uma probabilidade não-nula de uma parte da rede não tomar conhecimento de uma atualização (esse

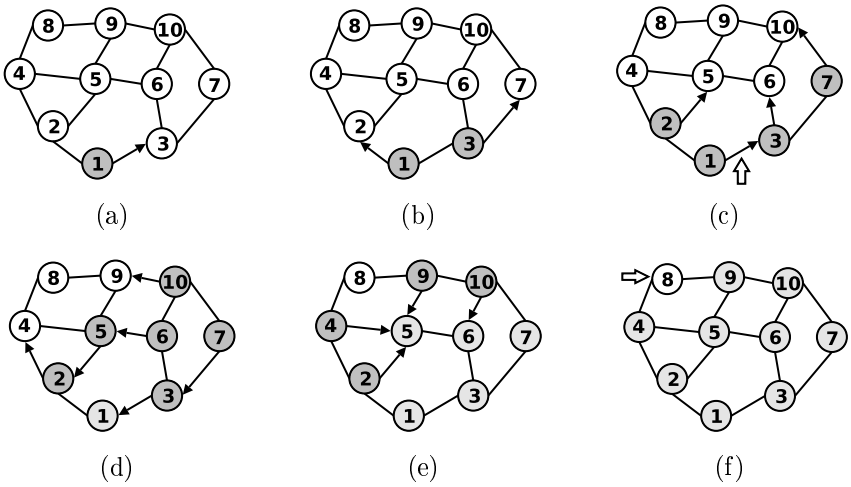


Figura 4.1: Comportamento do protocolo usando *push*

subconjunto é conhecido como *resíduo*). A variação de parâmetros como o k ou o tamanho do contador pode diminuir o tamanho provável do resíduo, mas não eliminá-lo.

Já no comportamento *pull*, em determinados momentos cada nó i da rede pergunta a um de seus vizinhos j se ele conhece alguma nova atualização. Caso j conheça, ele repassa esta atualização para i. Esse comportamento elimina o problema do resíduo, mas possui outros problemas. Por exemplo, ele utiliza uma quantidade constante de mensagens em um período de tempo para manter a rede atualizada, diferente do comportamento *push*, onde só ocorre a troca de mensagens quando existe de fato um rumor novo na rede. Em uma rede onde existam poucas atualizações o comportamento *pull* gera uma quantidade muito grande de mensagens inúteis.

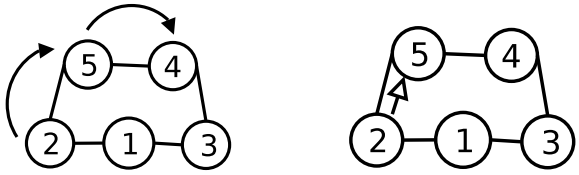
Além disso, no caso *pull* existe o compromisso entre o intervalo de tempo entre cada requisição para os vizinhos e a quantidade de mensagens que a rede irá gerar num dado intervalo de tempo.

É possível também utilizar um comportamento híbrido *push-pull*, onde utiliza-se primariamente o comportamento *push* para a disseminação de atualizações, usando o *pull* em intervalos de tempo mais longos apenas para garantir que não haverá resíduo na rede.

4.2 Alteração do modelo original para usar rumores

Nós utilizamos uma variação do método *pull* para disseminar as informações de experiência individual. Nessa variação tentamos minimizar o contato com informações de nós oportunistas desde a disseminação, de forma a não gastar mensagens disseminando informações comprometidas.

Assim, a disseminação de informação se dará da seguinte maneira: cada vez que um nó i requisitar serviço de roteamento de um nó j e esse fornecê-lo de forma justa, o nó i verificará se $R^t_{i(j)>0,5}$. Em caso positivo, i realizará um *pull* para j para obter novos relatos de experiência individual que ele já conheça. Essa restrição é importante para tentar manter as informações dadas por oportunistas fora das atualizações obtidas.



(a) Nó 2 manda mensagem para 4 através de 5

(b) Nó 2 pergunta para 5 se ele possui algum rumor novo

Figura 4.2: Comportamento do protocolo usando *pull*

Essa forma de disseminação de informação é representada na Figura 4.2 . Inicialmente temos o nó 2 enviando uma mensagem para o nó 4, roteando-a pelo nó 5 (Figura 4.2(a)). Ao verificar que a mensagem chegou corretamente ao seu destino (ou seja, o nó 5 forneceu serviço de forma justa), além do nó 2 atualizar a sua experiência individual com 5, ele irá verificar se 5 conhece alguma nova atualização (ou seja, uma operação *pull*), como mostra a Figura 4.2(b). Se o nó 5 não roteasse a mensagem por algum motivo, não haveria requisição de novas atualizações para ele. Isso tem a vantagem de evitar que um nó Sybil "envenene" a rede com informações falsas, sejam elas positivas sobre os outros Sybils quanto negativas sobre algum nó justo.

4.3 Impacto da topologia da rede substrato

Como o trabalho de Rocha [32] focava redes sobrepostas de roteamento, as simulações do modelo no artigo original (e nas simulações apresentadas até agora neste trabalho) assumiam que os nós oportunistas tinham as menores latências em comparação aos nós justos, o que fazia com que os nós justos os preferissem na hora de decidir por onde rotear seus pacotes. Esse comportamento causa o pior caso em uma rede de roteamento, pois a recusa em fornecer serviço dos oportunistas em posições centrais da rede de roteamento pode causar particionamento na rede.

Um exemplo de grafo de roteamento formado no início da execução do modelo dessa forma é apresentado na Figura 4.3. É possível ver que os nós oportunistas (os mais escuros) possuem muito mais ligações do que os outros nós na rede.

Entretanto, se considerarmos o caso médio da rede (onde nós oportunistas possuem latências similares às dos nós justos) teremos um comportamento diferente.

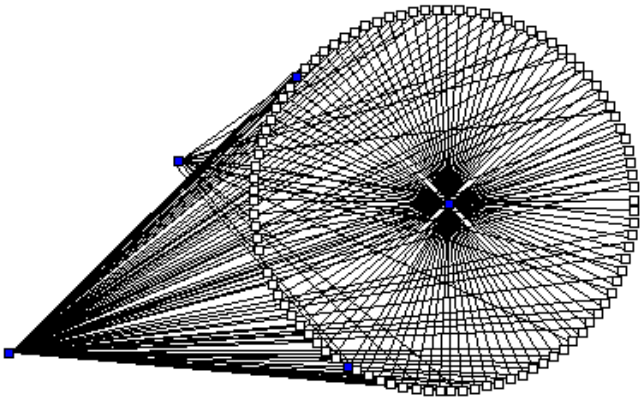


Figura 4.3: Grafo de roteamento com os oportunistas sendo melhores que os justos

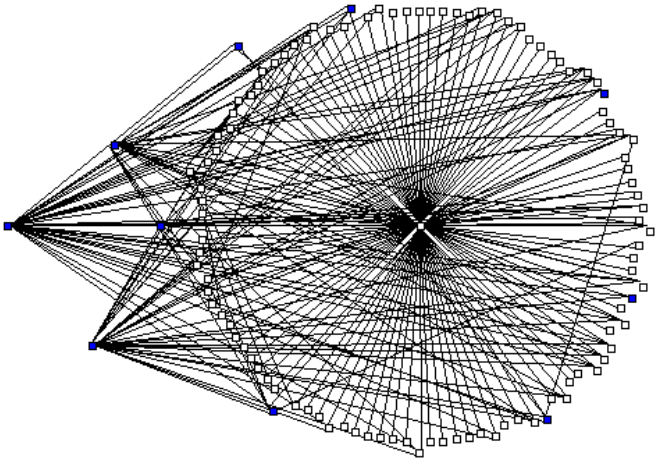


Figura 4.4: Grafo de roteamento com escolha aleatória de nós oportunistas

Como podemos ver na Figura 4.4, uma rede gerada de forma aleatória deixa de apresentar os nós oportunistas em posições privilegiadas em relação aos outros nós da rede. Nesse caso, o modelo original não apresenta a mesma eficácia na remoção de nós maliciosos, como pode ser visto na Figura 4.5. Isso se deve ao fato de que, por estarem em posições menos privilegiadas, os nós maliciosos são menos procurados pelos demais para fornecer serviços. Com menos interações a reputação dos nós maliciosos diminuirá com menor velocidade e portanto os nós justos levarão mais tempo para identificar esses nós.

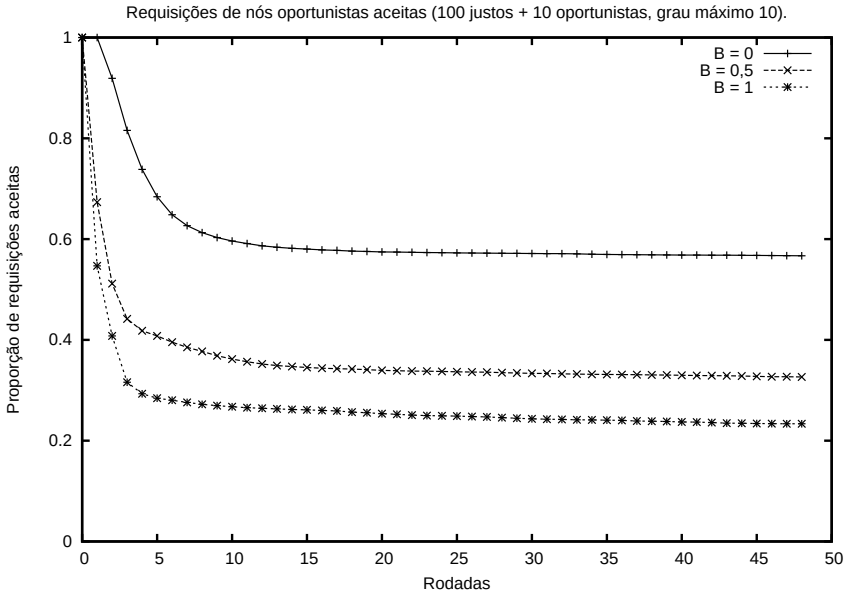


Figura 4.5: Serviço fornecido a oportunistas quando eles possuem posicionamento aleatório

4.4 Resultados experimentais

Realizamos alguns experimentos para verificar o impacto dessa nova alteração no desempenho do modelo de reputação. Esses experimentos foram realizados considerando uma rede com 100 nós justos e 10 nós oportunistas e $\alpha = 0,01$. Além disso, decidimos realizar estas simulações utilizando a escolha aleatória dos oportunistas dentre os participantes da rede, pois dessa forma obteremos o comportamento do protocolo de rumores num ambiente mais parecido com o de redes par-a-par de compartilhamento de arquivos, que é um dos focos deste trabalho (todavia, esse experimento ainda considera uma rede de roteamento sobreposta). Também limitamos o grau máximo de cada nó para 10 conexões.

4.4.1 Nós oportunistas

A Figura 4.6 apresenta uma comparação entre o modelo original, os modelos alterados e o modelo usando protocolo de rumores. Podemos observar que, as curvas apresentam comportamento bastante similar, devido ao uso apenas da experiência individual no cálculo de reputação.

Já a Figura 4.7 apresenta o comportamento dos modelos para $\beta = 0,5$. Nesse caso o modelo utilizando rumores conseguiu alcançar aproximadamente o mesmo nível de exclusão de oportunistas que o modelo original, aceitando apenas que cerca de 15% das requisições de oportunistas.

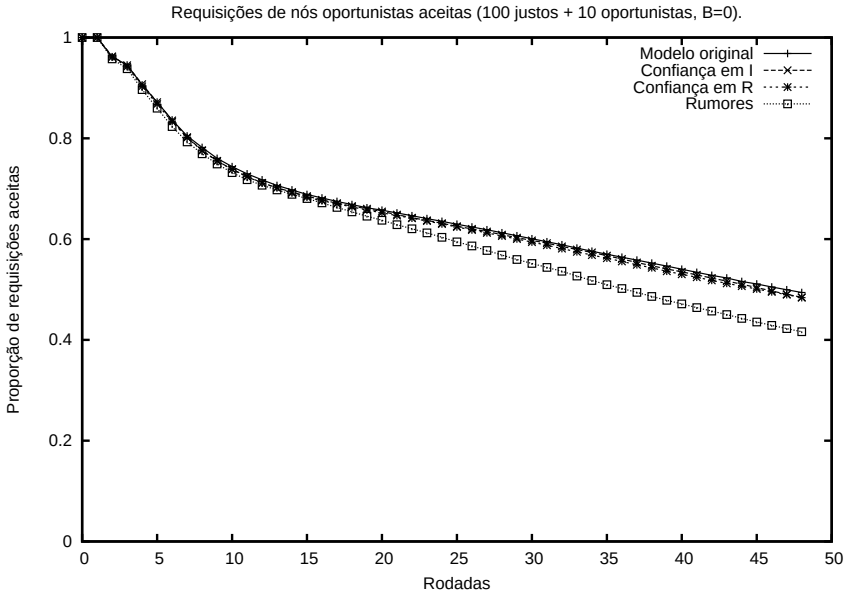


Figura 4.6: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 0$

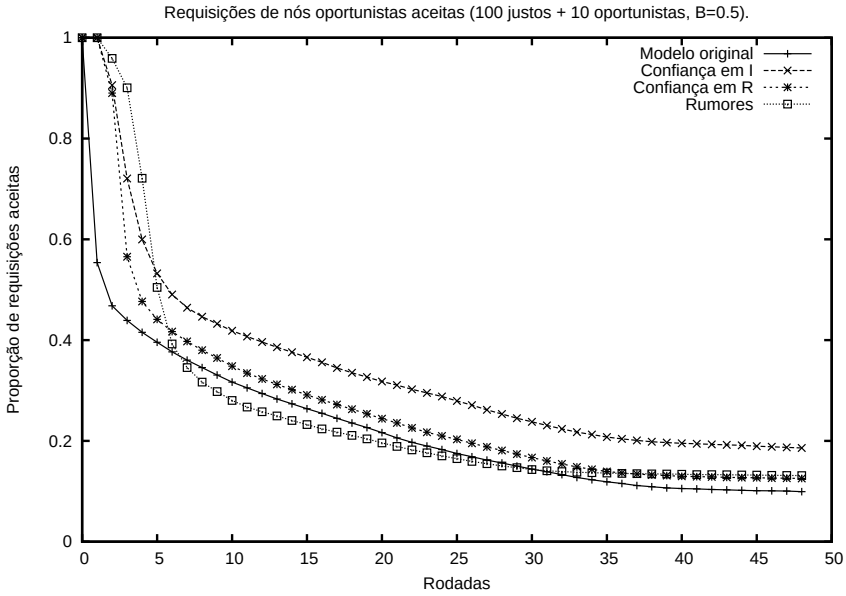


Figura 4.7: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 0,5$

O caso para $\beta = 1$ é apresentado na Figura 4.8. Podemos observar que o modelo usando rumores continua obtendo resultados próximos a aqueles obtidos com o modelo original, mesmo possuindo sem a manutenção de um estado global dos valores de experiência individual..

Para todos os valores de β apresentados o desvio padrão médio das curvas não

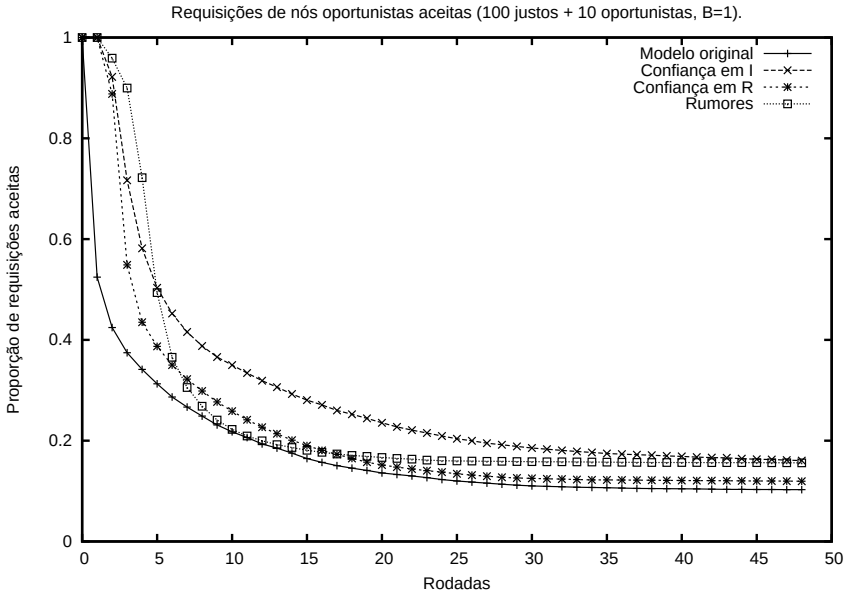


Figura 4.8: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 1$

excede $0,1$.

Podemos também utilizar a confiança baseada em experiência individual e em reputação para observar se esse tipo de restrição se comporta bem com o protocolo de rumores. Uma pequena alteração no modelo de reputações é feita no caso da confiança baseada em experiência individual: o critério usado passa a ser $I^t_{i(j)} > 0,5$, pois se fosse mantido o critério com $R^t_{i(j)}$ o modelo não conseguiria disseminar a informação para $\beta = 1$, pois nesse caso o aumento da experiência individual após uma transação bem sucedida não ajudaria no aumento do valor de reputação, e portanto os nós nunca efetuariam a operação *pull* por atualizações.

Por brevidade não apresentaremos o resultado para $\beta = 0$, pois nesse caso as alterações, que visam modificar a forma que as opiniões de outros nós é utilizada no calculo de reputação, não apresentam mudanças significativas no desempenho do sistema.

A Figura 4.9 apresenta o comportamento dos modelos para $\beta = 0,5$. Podemos observar que o modelo de rumores com confiança baseada em reputação apresenta o mesmo desempenho que o modelo de rumores simples, com o modelo de rumores com confiança baseada em experiência individual apresentando um resultado quase tão bom quanto quanto o deles. Contudo, as restrições impostas pelos próprios modelos não permitem que eles alcancem o mesmo desempenho do modelo original.

O comportamento para $\beta = 1$ (Figura 4.10) apresenta-se muito similar ao caso com $\beta = 0,5$. Para os dois valores de β o desvio padrão médio das curvas é menor que $0,1$.

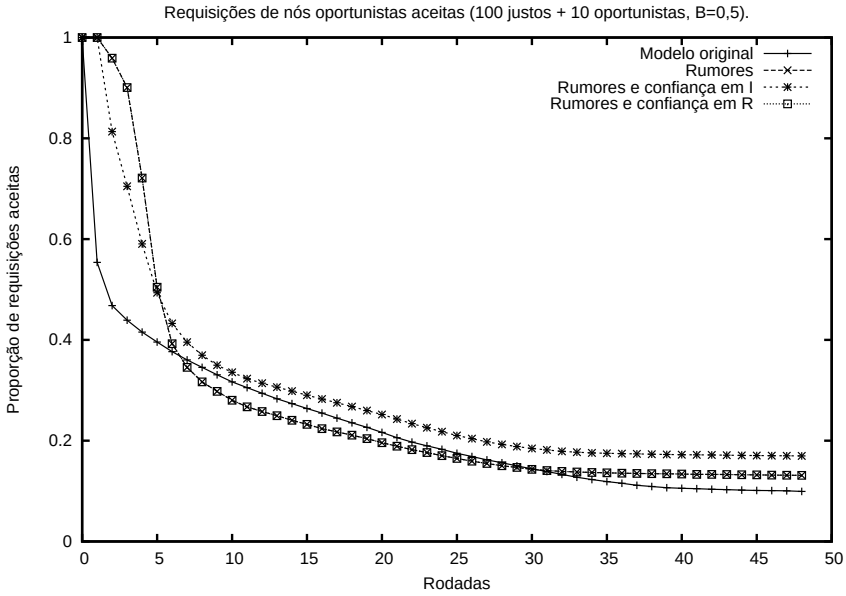


Figura 4.9: Serviço fornecido a nós oportunistas com modelo de rumores simples e rumor utilizando confiança na experiência individual e reputação com $\beta = 0,5$

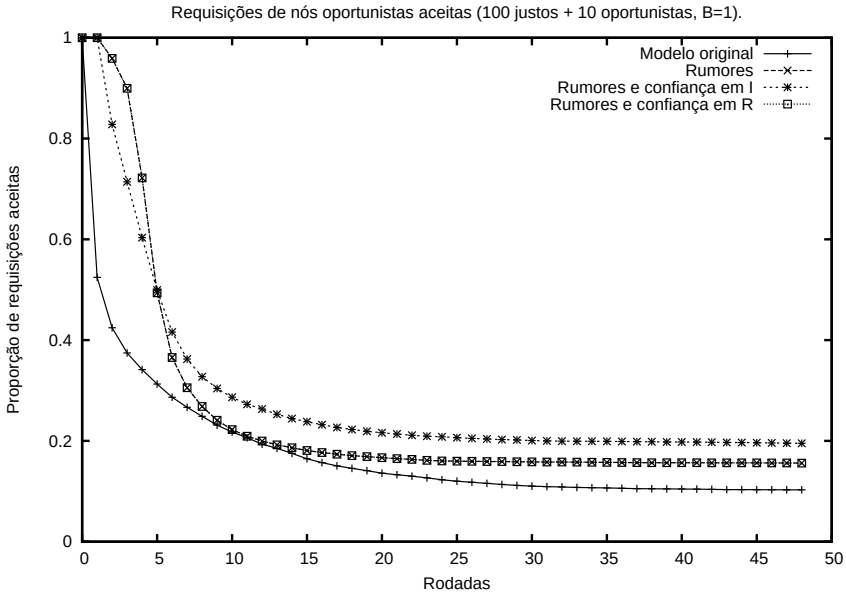


Figura 4.10: Serviço fornecido a nós oportunistas com modelo de rumores simples e rumor utilizando confiança na experiência individual e reputação com $\beta = 1$

4.4.2 Nós Sybil

No caso contra nós Sybil, o comportamento para $\beta = 0$ continua sendo igual ao apresentado para nós oportunistas, e portanto não apresentaremos gráfico para esse caso.

Para o caso de $\beta = 0,5$ apresentado na Figura 4.11, temos a versão com rumores

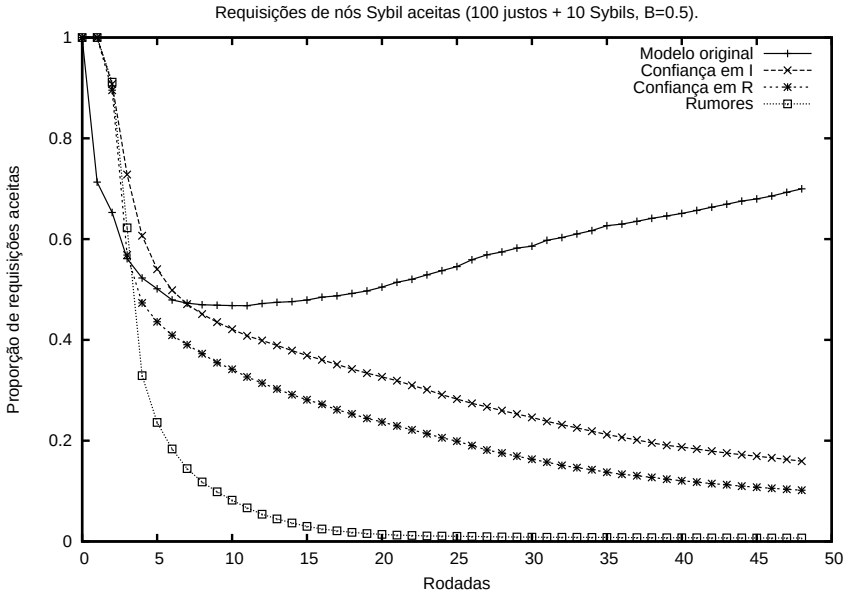


Figura 4.11: Serviço fornecido a nós Sybil no modelo original e no modelo com rumores para $\beta = 0,5$

sem apresentar o aumento na proporção de requisições aceitas de Sybil, além de obter um ótimo desempenho na exclusão de nós Sybil, bloqueando quase todas as requisições feitas por esses nós. Isso significa que, além de isolar as informações fornecidas pelos nós Sybil, o protocolo de rumores consegue atualizar a rede com os mais recentes valores de experiência individual em uma velocidade adequada. As curvas para rumores com confiança baseada em experiência individual e em reputação não conseguem alcançar a mesma velocidade na exclusão de nós Sybil, mas apresentam tendência a continuar melhorando seus resultados gradativamente ao fim da simulação. Para o caso de $\beta = 1$, apresentado na Figura 4.12, podemos verificar o mesmo comportamento descrito acima. O desvio padrão médio das curvas alteradas é menor do que $0,5$ para todos os valores de β experimentados.

Porém, existe a possibilidade que os nós Sybil aceitem algumas poucas requisições apenas para que os nós justos façam um *pull* de suas informações adulteradas sobre o comportamento dos Sybils. Para evitar que esse tipo de comportamento afete a rede de forma negativa podemos utilizar a confiança baseada em experiência individual e reputação, apresentadas anteriormente. Dessa forma, além de restringir de quem se obtém os dados, também se restringe quais informações serão utilizadas no cálculo da reputação.

A seguir apresentaremos o comportamento do modelo usando apenas o protocolo de rumores, o protocolo de rumores e confiança baseada em experiência pessoal e o protocolo de rumores com confiança baseada em reputação, para o caso onde os Sybils

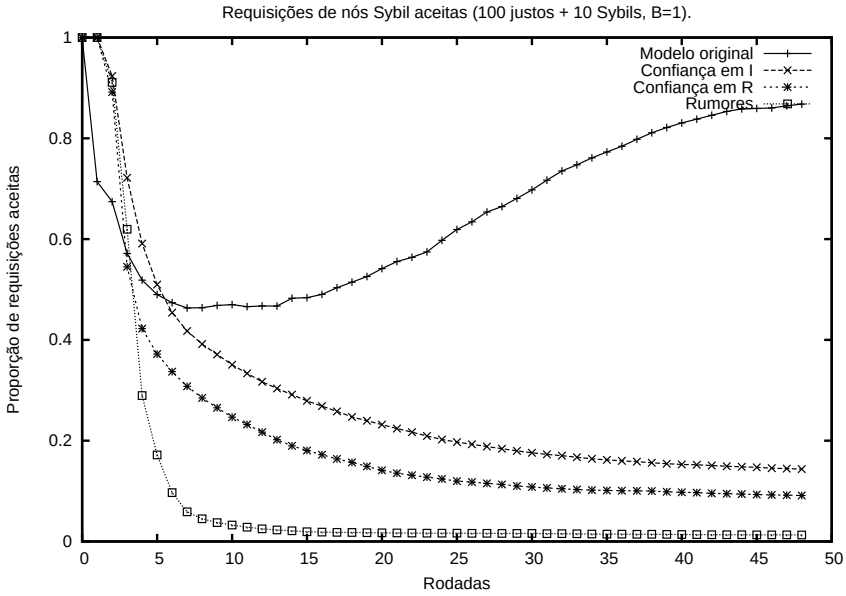


Figura 4.12: Serviço fornecido a nós Sybil no modelo original e no modelo com rumores para $\beta = 1$

fornecerão parte do serviço para adulterar os dados da rede. Aqui cada um dos nós Sybil irá aceitar uma requisição com probabilidade de 10%. Consideramos esse o pior caso possível pois tendo 10 nós Sybil, aceitar até 10% faz a entidade maliciosa responsável pelos nós Sybil fornecer potencialmente o mesmo serviço que um nó justo, o que não é desejável para ele. O gráfico com o comportamento dos modelos para $\beta = 0$ não será apresentada por não apresentar alterações, pois ,como não utiliza informações de pares, essa configuração não é afetada por um ataque Sybil.

A Figura 4.13 apresenta esse caso para $\beta = 0,5$. É possível notar que o modelo de rumores simples, após parte da simulação, volta a aceitar requisições de Sybils, pois agora eles conseguem periodicamente alimentar a rede com suas informações adulteradas. Contudo, os modelos com rumores e confiança em experiência individual e reputação se mantém imunes a esse efeito causado pelos Sybils, com uma boa vantagem da confiança baseada em reputação no desempenho da exclusão de nós Sybil.

O comportamento dos modelos com $\beta = 1$ é apresentado na Figura 4.14. Aqui o modelo de rumores simples volta a aceitar requisições de nós Sybil de forma um pouco mais acentuada, devido ao maior peso concedido às opiniões de outros nós. Já os modelo de rumores com confiança baseada em reputação e em experiência individual continuam apresentando bom desempenho, não permitindo que informações adulteradas geradas por nós Sybil causem danos ao sistema de reputações. O desvio padrão médio nesses casos permanece menor do que $0,5$ para o protocolo de rumores e confiança (tanto em reputação quanto para experiência individual). Já no caso de apenas rumores o

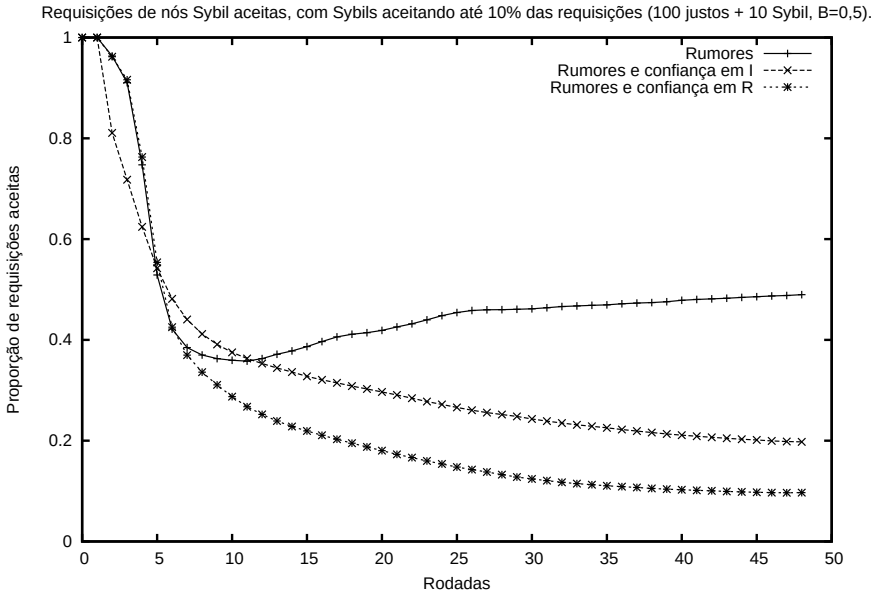


Figura 4.13: Serviço fornecido a nós Sybil com modelo de rumores simples e rumores com confiança na experiência individual e na reputação, com $\beta = 0,5$ e Sybils aceitando até 10% das requisições

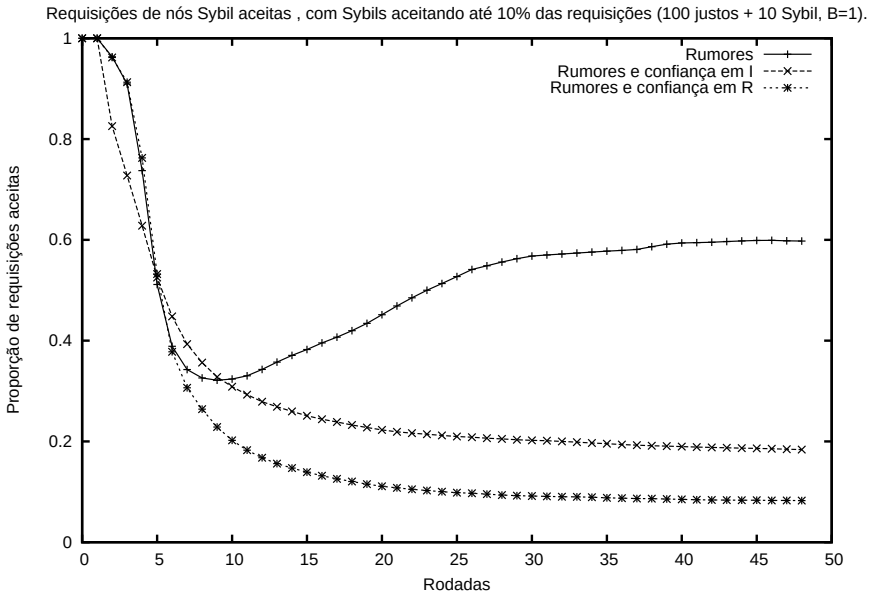


Figura 4.14: Serviço fornecido a nós Sybil com modelo de rumores simples e rumores com confiança na experiência individual e na reputação, com $\beta = 1$ e Sybils aceitando até 10% das requisições

desvio padrão médio é muito mais alto, chegando a aproximadamente $0,45$ no fim dos experimentos. Esse aumento do desvio padrão ocorre também (mesmo que não tão acentuadamente) para o modelo original frente a um ataque Sybil. Todavia o

importante nesse caso é notar a tendência de nós justos voltarem a aceitar requisições de nós Sybil quando eles apresentam esse comportamento..

4.5 Sumário

Neste capítulo avaliamos o uso de um protocolo de rumores para tratar a manutenção do estado global do modelo original de forma mais suave no que diz respeito à quantidade de mensagens de atualização de estado trafegadas pela rede. Utilizamos também as modificações ao modelo propostas para combater ataques Sybil e mostramos que, ainda é possível identificar e excluir alguns nós Sybil definitivamente (ou seja, sem permitir que eles voltassem a ter suas requisições aceitas por nós justos) com um bom desempenho. Além disso, verificamos que essa alteração não atrapalha o modelo de reputações no combate a nós oportunistas que não se utilizem de conluio para enganar o sistema.

Capítulo 5

A rede BitTorrent

Quando um determinado conteúdo é disponibilizado através de uma rede cliente-servidor, toda a carga gerada pelo *download* desse conteúdo será atribuída a um único servidor. Para diminuir esta carga gerada no servidor de conteúdo pode-se utilizar uma rede par-a-par (*peer-to-peer, P2P*) de compartilhamento de arquivos, de modo que os pares que estão obtendo o conteúdo também auxiliem na distribuição do mesmo.

Uma rede par-a-par muito utilizada atualmente na disponibilização de conteúdo na Internet é o *BitTorrent* [11], muito utilizado na disponibilização de arquivos grandes, como distribuições Linux. Vários trabalhos tiveram essa rede como tema de estudo e defendem que ela é altamente escalável, resistente a fenômenos como *flash crowds* e que oferece boa qualidade de *download* aos usuários [5, 30].

O *BitTorrent* utiliza um esquema onde cada interessado no conteúdo compartilha as partes obtidas desse arquivo tão logo as obtenha, ou seja, não é necessário que se complete o *download* do arquivo para compartilhá-lo. Além disso, os pares interessados no mesma arquivo "trocam" as partes obtidas uns com os outros, de modo a diminuir a carga no servidor original e aumentar a velocidade dos *downloads*, visto que cada par obtém partes do arquivo de diversas fontes.

O protocolo do *BitTorrent* possui políticas aplicadas à troca de partes para impedir que pares mal-intencionados obtenham partes do arquivo sem fornecer participantes para os outros pares da rede (ou seja, um nó oportunista ou *free-rider*), visto que colaboração entre os pares é que permite o bom desempenho da rede. Entretanto, as políticas atualmente aplicadas não são suficientes para impedir que pares oportunistas tirem vantagem da rede [5].

Considerando que o modelo de reputação apresentado por Rocha [32] tenta justamente fatorar a troca de serviço sentre nós, nossa proposta é aplicar esse modelo em conjunto com as políticas do próprio *BitTorrent* na tentativa de coibir ainda mais o comportamento oportunista na rede.

5.1 Componentes de uma rede BitTorrent

Para compreender o funcionamento do protocolo do *BitTorrent* é importante familiarizar-mo-nos com alguns componentes e termos definidos pelo mesmo. Como existem várias implementações desse protocolo, às vezes um mesmo componente possui mais de uma denominação; essas diferentes denominações também serão apresentadas.

- **Rastreador ou *tracker*:** é um elemento centralizado na rede que funciona como um "ponto de encontro" para os nós interessados em um mesmo arquivo. O rastreador guarda algumas informações sobre cada participante para fins de registro.
- **Pares, *downloaders* ou *leechers*:** são os participantes da rede que desejam o arquivo completo.
- **Sementes, *seeds* ou *seeders*:** são participantes que já possuem o arquivo completo, mas continuam participando da rede apenas realizando o *upload* para outros pares. Atualmente não existe um mecanismo de incentivo para que uma semente continue conectada, apesar delas terem um papel importante no bom funcionamento da rede. Normalmente, entretanto, o interessado na distribuição do arquivo mantém ao menos uma semente ativa na rede.
- ***Torrent*:** o conjunto de pares e sementes ligados a um mesmo rastreador e que compartilham um mesmo conteúdo.
- **Blocos:** um arquivo disponibilizado através do BitTorrent é dividido em blocos de tamanho fixo, que em geral variam entre 256 KB e 2 MB, dependendo do tamanho total do arquivo.
- **Partes ou sub-blocos:** um bloco é formado por um conjunto de partes de 16 KB.
- **Arquivo Torrent:** é um arquivo que contém as informações necessárias para que um par participe de um *torrent*, entre elas o endereço do rastreador, tamanho do arquivo desejado, um valor de *hash* do arquivo completo e um valor de *hash* de cada um dos blocos que compõem este arquivo, para verificação de integridade.

5.2 Funcionamento da rede BitTorrent

O funcionamento do *BitTorrent* pode ser analisado em termos da disponibilização de conteúdos, da política que um nó utiliza para escolher qual bloco ele requisitará de outro

par, de como é realizada a reciprocidade no compartilhamento de blocos, da escolha de quais pares recebem serviço e de como evitar a oferta de serviço a nós oportunistas. Essas partes do protocolo são apresentadas a seguir.

5.2.1 Disponibilização de conteúdo

Diferente de redes de compartilhamento de arquivos como Gnutella [31] ou eDonkey[1], o BitTorrent não oferece recursos de meta-busca[2]. Quando alguém deseja disponibilizar um determinado conteúdo através do BitTorrent, ele deve gerar um arquivo torrent para esse conteúdo e publicá-lo em algum ponto da rede. Existem vários sítios WWW, como por exemplo *Torrentspy*[3] e *Mininova*[4], que servem de repositório de arquivos torrent para variados tipos de conteúdo.

Os interessados em um conteúdo devem obter o arquivo torrent correspondente a ele. Utilizando esse arquivo, o par pode entrar em contato com o rastreador, que responde com o endereço de um conjunto aleatório de pares e sementes participantes do mesmo *torrent*.

De posse desses contatos, o novo par estabelece conexão com um subconjunto deles (o número exato depende do tamanho do torrent, mas em geral não excede 70). Para evitar a renegociação da conexão, o par não fecha essas conexões mesmo que não haja tráfego nelas.

A partir desse ponto a troca de arquivos pode se iniciar de fato.

5.2.2 Escolha de blocos

Dependendo do momento no processo de *download*, um par escolhe qual bloco irá requisitar de um outro par ou semente de uma forma diferente. Essas políticas de escolha são as seguintes:

- **Escolha aleatória:** um par i escolhe uma das partes disponibilizadas pelo outro par ou semente j de forma aleatória. Essa escolha aleatória só é feita enquanto i não possuir nenhum bloco completo, para tentar completar pelo menos um bloco o quanto antes.

- **Mais raro primeiro:** quando o par i tem pelo menos um bloco completo, ele passa a requisitar aqueles blocos que estão menos replicados entre os pares que

[1] http://www.edonkey2000.com

[2] Busca por palavra chave para localizar conteúdo, feita através da própria rede de compartilhamento

[3] www.torrentspy.com

[4] www.mininova.org

ele conhece. Isso é feito para tentar impedir o *problema do último bloco*, onde o fornecedor original abandona a rede antes que pelo menos uma cópia completa do arquivo seja realizada.

- **Fim de jogo:** quando faltam poucos blocos para finalizar o arquivo, o par faz várias requisições do mesmo bloco paralelamente, na tentativa de não atrasar a finalização do arquivo por ter requisitado o bloco de um par ou semente lento.

5.2.3 Política de reciprocidade (*tit-for-tat*)

Para evitar que usuários oportunistas utilizem o sistema, cada par envia blocos apenas para nós que também fornecem blocos para ele. Sementes, que não requisitam mais blocos de nenhum outro nó, não buscam reciprocidade na alocação de banda.

Para um par otimizar a sua velocidade de *download* é importante que ele decida da melhor forma para quais pares ele vai realizar a reciprocidade com a banda de subida. Para decidir isso, o *BitTorrent* utiliza um protocolo de bloqueio.

5.2.4 O algoritmo de bloqueio (*choking algorithm* no original)

Inicialmente, todas as conexões de um par estão bloqueadas (*choked*, no original). Em um dado momento um par pode desbloquear (*unchoke* no original) até 5 conexões, ou seja, um par realiza *upload* para até 5 outros pares ao mesmo tempo.

A escolha de quais pares serão desbloqueados em um dado momento é feita da seguinte forma: tenta-se garantir a reciprocidade a todos os pares (não sementes) que não estão bloqueando aquele nó, dando preferência aos pares que oferecem a melhor taxa de *download*. Dessa forma, o conjunto de pares desbloqueados por um nó i não necessariamente é igual ao conjunto de pares que desbloqueiam i.

As sementes escolhem quais pares desbloquear avaliando quais nós podem realizar um *upload* mais veloz. Isso ocorre para tentar fornecer a maior quantidade de blocos possíveis no menor intervalo de tempo, aumentando a disponibilidade de blocos na rede.

Para evitar que haja bloqueios e desbloqueios sucessivos e muito rápidos (comportamento chamado no protocolo de *fibrilação*), que impeçam a estabilização de uma conexão, a escolha de quais conexões desbloquear é feita a cada 10 segundos.

5.2.5 O desbloqueio otimista

Para testar novas conexões ainda inativas (além de conceder a nós recém-chegados a chance de obter seu primeiro bloco) cada par (ou semente) i possui sempre uma

conexão desbloqueada com um outro par aleatório j, não importando se j desbloqueou i ou se a taxa de *download* que i tem com j é boa.

A conexão desbloqueada otimisticamente é trocada a cada 30 segundos para permitir que a conexão se estabilize, além de dar tempo para um par recém-chegado obter pelo menos um bloco. Se no momento da troca do desbloqueio otimista o atual desbloqueio apresentar uma boa taxa de download, ela pode ser mantida como um desbloqueio comum.

Essa liberação de banda de forma indiscriminada é uma das fontes reconhecidas de injustiça no BitTorrent, pois permite que um nó oportunista obtenha blocos livremente. Qiu [30] afirma que um nó oportunista dependendo apenas de desbloqueios otimistas ainda obtém 20% da taxa de *download* máxima possível.

5.2.6 Anti-Esnobe

Quando um nó j desbloqueia um no i, mas após 60 segundos de transferência i não obteve nenhuma parte completa de j, diz-se que o nó j está *esnobando* (*snubbing*, no original) o nó i. Quando um par se sente esnobado, ele bloqueia a conexão com o nó esnobe e não a desbloqueia, exceto em caso de desbloqueio otimista. Já uma semente não desbloqueia um nó que ele considere esnobe nem mesmo em caso de desbloqueio otimista.

Um par i só deixa de considerar um nó j esnobe se j mandar pelo menos uma parte (ou seja, 16 KB de dados) para i em um determinado espaço de tempo (em geral 45 segundos). Uma semente não muda sua opinião sobre o comportamento esnobe de outros pares.

5.3 Utilizando reputação com o BitTorrent

Para identificar e isolar pares oportunistas o *BitTorrent* utiliza a política de anti-esnobe. Para garantir que o comportamento de um nó é oportunista ele utiliza o valor médio da velocidade de transmissão durante 60 segundos, se depois desse tempo o nó continuar não fornecendo serviço ele será excluído da rede.

É possível utilizar uma política de reputação no lugar do anti-esnobe para identificar nós oportunistas. Uma das maiores vantagens de se utilizar a reputação nesse caso seria a difusão da informação de quais nós são oportunistas para os outros participantes da rede, pois o anti-esnobe utiliza apenas informações locais para essa identificação.

Porém, algumas alterações se tornam necessárias para poder se utilizar um mecanismo de reputação nesse ambiente. Inicialmente, o que caracteriza o comportamento oportunista em um par não é tão bem identificável no *BitTorrent* quanto em uma rede

de roteamento sobreposta. Enquanto na rede sobreposta o comportamento oportunista se caracteriza pelo não fornecimento de serviço, em uma rede de compartilhamento de arquivos ela poderia ser não só a recusa no fornecimento do arquivo como o fornecimento desse arquivo de forma inadequada (como por exemplo fornecer pouca banda para *upload*).

Decidimos utilizar uma política de avaliação de justiça mais atenta à troca de blocos do que com a alocação de banda. Alguns trabalhos sugerem que políticas de justiça aplicadas à troca de blocos sejam mais efetivas [6]. Em nossa política um nó A é considerado justo por B(e portanto terá seu valor de experiência individual incrementado) quando fornecer um bloco inteiro para ele.

Já o comportamento injusto será identificado de forma similar ao anti-esnobe. Quando um nó A desbloquear uma conexão com B mas não fornecer nenhum dado para ele em um determinado intervalo de tempo, B diminuirá o valor da experiência individual que tem com A. Como o modelo baseado em reputação apresenta uma queda gradativa de confiança (diferente do anti-esnobe, onde a relação é cortada com um nó após identificar-se o primeiro sinal de oportunismo dele), utilizamos um tempo menor para avaliar um nó como oportunista, no caso 30 segundos. Além disso, essa avaliação será refeita a cada 10 segundos após a primeira avaliação de A como oportunista até que ele forneça dados para B. Isso é feito para diminuir o tempo necessário para se excluir um nó oportunista da rede.

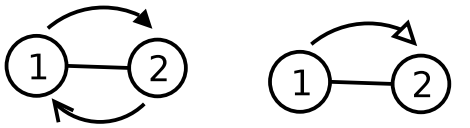
(a) Nó 1 manda mensagem para 3 através de 2

(b) Nó 1 altera a experiência que tem com 2

Figura 5.1: Avaliação de justiça em redes de roteamento

Um ponto interessante a se notar também é quem será avaliado pelo fornecimento de serviço em cada tipo de rede. A Figura 5.1(a) apresenta o comportamento de uma rede de roteamento sobreposta onde o nó 1 manda uma mensagem para o nó 3 (**??**). Nesse caso quem fornece serviço para 1 é o nó 2, que efetuará o roteamento da mensagem, de modo que 1 modificaria sua experiência pessoal com 2 (5.1(b)).

Já no caso do compartilhamento de arquivos, como podemos ver na Figura 5.2, quando um nó 1 requisita um arquivo (ou parte dele) de um nó 2 e ele o fornece para 1 (5.2(a)), então 1 modificaria sua experiência individual com 2 (5.2(b)).



(a) Nó 1 manda pede dados de 2, 2 envia dados para 1

(b) Nó 1 altera a experiência que tem com 2

Figura 5.2: Avaliação de justiça em redes de compartilhamento de arquivos

5.4 Experimentos

Alteramos o simulador de Rocha para que ele funcionasse como uma rede *BitTorrent*, e não como uma rede de roteamento. Implementamos o protocolo como ele é descrito neste capítulo, sendo que apenas o modo fim de jogo não foi implementado por motivo de simplicidade, visto que ele tem como objetivo garantir que um *download* não demore muito para terminar sua última parte e nossa simulação se interessa em descobrir se nós oportunistas são de fato excluídos, e não fazer medições de desempenho de *downloads*. Em nossa simulação cada nó apresenta valores de banda de subida e descida fixos, e busca otimizar a alocação de sua banda de subida de forma a maximizar o uso de sua banda de descida (ou seja, tenta obter o máximo de serviço com o mínimo de comprometimento de recursos próprios). A simulação considera que existe inicialmente apenas uma semente na rede, ou seja, apenas um nó possui o arquivo completo. Todos os outros nós iniciam sem nenhuma parte.

É válido também ressaltar que a descrição apresentada nesse capítulo refere-se ao protocolo *BitTorrent* como apresentado em sua documentação oficial, mas que essa documentação apresenta apenas a base do protocolo, sendo que os desenvolvedores são encorajados a otimizar detalhes onde eles acharem adequado.

Como a maioria de trabalhos sobre o *BitTorrent* utilizam a coleta de dados reais para avaliação de desempenho do mesmo [21, 29] e o nosso simulador não considera detalhes de nível mais baixo, como por exemplo congestionamento da rede, torna-se difícil utilizar algum daqueles trabalhos para validar o simulador. Porém é possível ver nos resultados que obtivemos alguns dos comportamentos esperados do *BitTorrent*. Por exemplo, a Figura 5.3 apresenta a proporção de blocos obtida por pares e que foram obtidas através de sementes e através de outros pares. Podemos ver que no início o primeiro bloco a ser obtido terá obrigatoriamente de vir da semente original, pois ela é a única que possui partes do arquivo. Porém, a partir do momento que alguns pares possuem partes para compartilhar a proporção de partes obtidas a partir de outros pares começa a aumentar. Como a banda entre pares será muito maior que a banda da semente (por causa da grande quantidade de pares contra apenas uma semente)

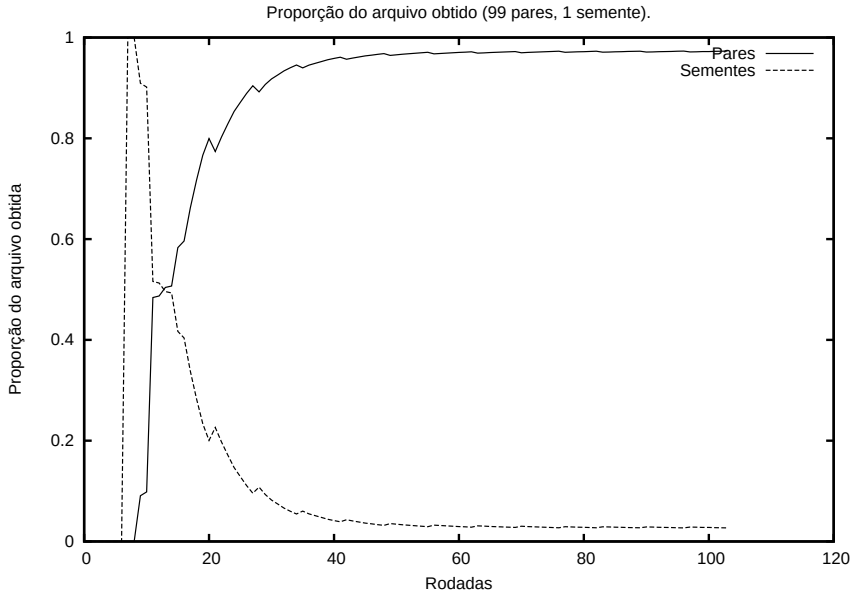


Figura 5.3: Proporção do arquivo obtido através de pares e sementes

a proporção de partes obtidas por sementes tende a diminuir e a de partes obtidas por outros pares tende a aumentar. Esse é o comportamento esperado do protocolo *BitTorrent*, onde a carga atribuída ao fornecedor inicial do arquivo é pequena, pois essa carga é repassada para os pares.

5.4.1 Rede com nós oportunistas

Agora veremos o comportamento da rede *BitTorrent* original quando temos nós oportunistas participando da rede. A Figura 5.4 apresenta a proporção do arquivo obtida por nós justos e por nós oportunistas em uma rede comum. O comportamento dos oportunistas nesse caso é bastante simples, similar ao apresentado no exemplo de redes de roteamento no Capítulo 2, com os nós tentando obter o máximo de serviço possível sem oferecer nada em troca. Podemos observar que o anti-esnobe consegue diminuir drasticamente a quantidade de serviço fornecida a nós oportunistas nesse ambiente. Mas é interessante notar que, após todos os pares terminarem o *download* e tornarem-se sementes (o que ocorre aproximadamente na rodada 700), a proporção de blocos obtidos por oportunistas aumenta. Isso ocorre porque agora não existe mais concorrência de nós justos para obter banda das sementes de forma que, se os oportunistas não foram considerados esnobes por todas as sementes que conhecerem, eles ainda poderão obter blocos do arquivo desejado sem qualquer custo.

Porém, se os nós oportunistas utilizarem técnicas um pouco mais sofisticadas, o anti-esnobe passa a não ter um comportamento tão bom. Um nó não é considerado

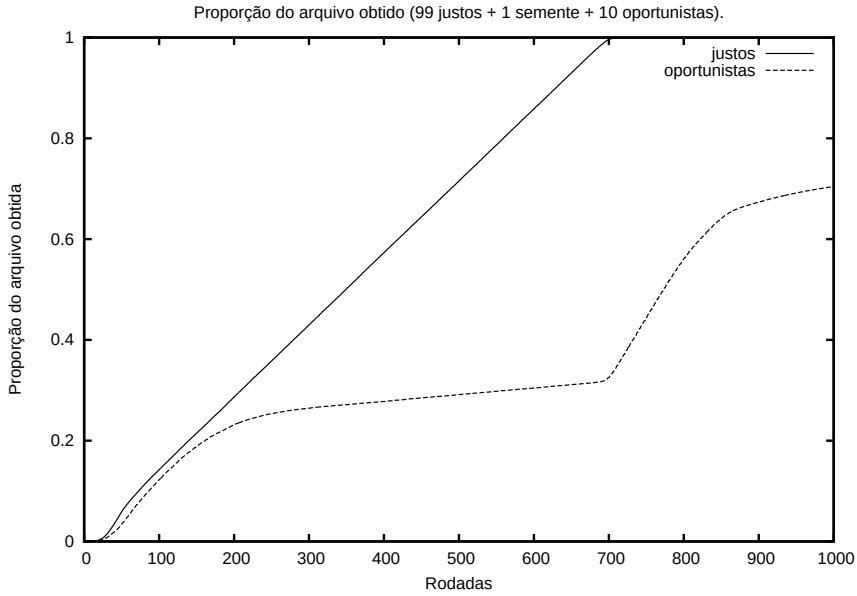


Figura 5.4: Proporção do arquivo obtido por oportunistas e justos numa rede *BitTorrent* tradicional

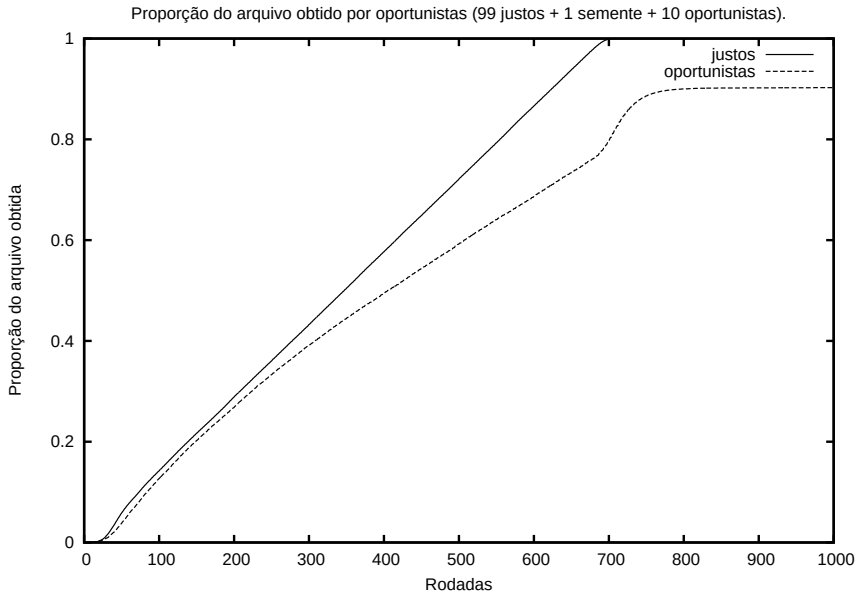


Figura 5.5: Proporção do arquivo obtido por justos e por oportunistas que compartilham o mínimo possível 10% do tempo

esnobe se realizar *upload* a uma velocidade de pelo menos 300 bps (o suficiente para mandar 16 KB em um minuto). Sendo essa uma velocidade razoavelmente pequena, se um oportunista decidir realizar *uploads* a essa velocidade em determinados momentos para outros nós, não só ele poderá obter algumas partes a mais no processo de download normal (pois os nós justos tentarão realizar reciprocidade nesse *upload*), como poderão

se manter como não esnobes e, caso os seus pares se tornem sementes, poderão obter dados sem fornecer mais serviço (já que as sementes não identificam novos esnobes). A Figura 5.5 apresenta o *BitTorrent* comum com os nós oportunistas fazendo uploads mínimos para pares com uma chance de 10%, e apresenta a proporção do arquivo obtida por nós justos e oportunistas. Podemos notar que o anti-esnobe passou a não ser mais tão eficiente na exclusão de nós oportunistas, pois apesar de conseguir barrar os oportunistas quando eles alcançaram uma proporção próxima a 90% do arquivo, eles obtiveram essa proporção em bem menos tempo do que deveriam e podem obter o resto do arquivo escolhendo novos pares ou sementes para obter serviço ou entrar e sair da rede, de modo a parecerem recém-chegados (procedimento conhecido como *whitewash*).

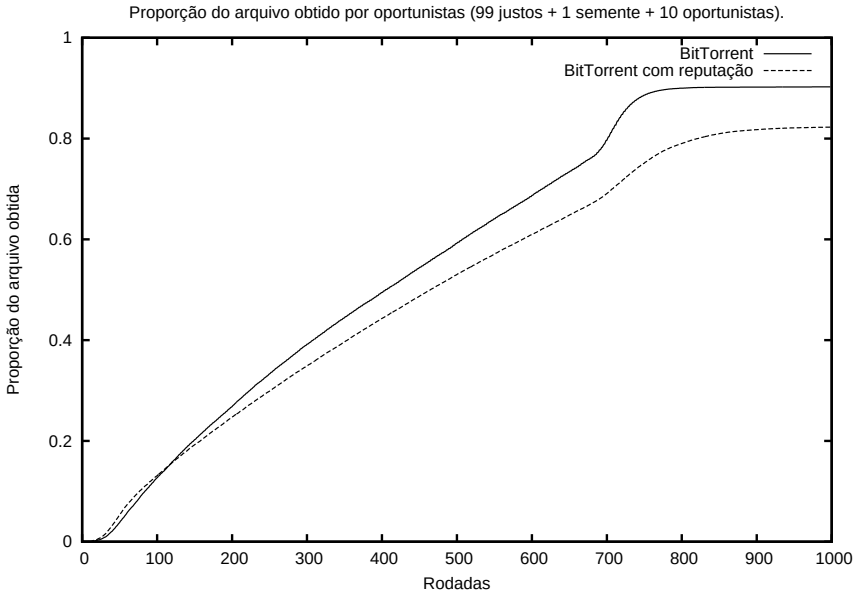


Figura 5.6: Proporção do arquivo obtido por oportunistas que compartilham o mínimo possível 10% do tempo para o BitTorrent tradicional e com reputação

Já a Figura 5.6 apresenta o mesmo caso, porém utilizando o modelo de reputações para identificar os nós oportunistas. Podemos notar que existe uma melhora em relação à proporção do arquivo obtida por oportunistas, mas ainda assim nada muito significativo. Isso se dá porque a diminuição gradativa da confiança em um nó prevista no modelo de reputações não consegue excluir nós oportunistas tão rapidamente quanto o anti-esnobe, onde ao primeiro sinal de oportunismo o nó já é excluído da rede. Apesar dessa velocidade menor de reação ser compensada pelas opiniões (depoimentos) de outros nós (afinal, o resultado obtido foi melhor do que o do *BitTorrent original*), esse resultado ainda poderia ser melhor.

Com isso em mente, decidimos alterar mais uma vez o modelo de forma a conseguirmos uma queda mais acentuada do valor da experiência individual a cada interação mal sucedida. Através da Equação 2.1, que nos apresentou as fórmulas para o cálculo da experiência individual, podemos ver que apesar da multiplicação da penalidade por um fator n^2 o decréscimo do valor de $I^t_{i(j)}$ é essencialmente aditiva. Sistemas de controle bem sucedidos, como o controle de congestionamento do protocolo TCP, usam formas de crescimento aditivo/redução multiplicativa, consideradas mais estáveis [22].

Decidimos então alterar a fórmula para aquela apresentada na Equação 5.1. Nessa nova fórmula temos que o decréscimo de $I^t_{i(j)}$ é dado pela multiplicação por um fator baseado em um novo parâmetro γ, escolhido pelo projetista. Dessa forma, não importando quão alta seja o valor da experiência individual de um par, qualquer comportamento oportunista será punido de forma mais dura que no modelo original. A expressão não usa simplesmente o γ, mas leva também em consideração o serviço parcial ($\frac{p}{r} > 0$). Assim sendo, no pior caso o fator será γ, mas pode crescer até um valor mais próximo de 1 caso o serviço parcial for alto, o que diminuirá a redução da experiência individual.

$$I^t_{i(j)} = \begin{cases} min(I^{t-1}_{i(j)} + \alpha, 1) & se\ p = r \\ \\ max(I^{t-1}_{i(j)} * (((1-\gamma) * \frac{p}{r}) + \gamma), 0) & se\ S_{i(j)} - S_{j(i)} > 0\ e\ p \neq r\ e\ 0 \leq \gamma \leq 1 \end{cases} \tag{5.1}$$

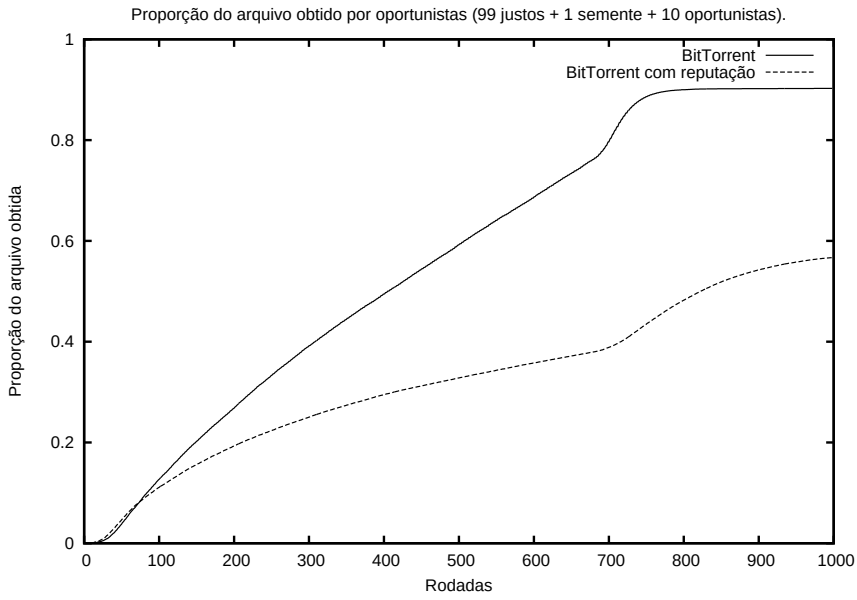


Figura 5.7: Proporção do arquivo obtido por oportunistas que compartilham o mínimo possível 10% do tempo para o BitTorrent tradicional e com reputação com $\gamma = 0,75$

A Figura 5.7 apresenta a proporção do arquivo obtida por nós justos e oportunistas usando o modelo de reputação com a alteração descrita e $\gamma = 0,75$. Podemos ver que o sistema reage melhor aos oportunistas, negando-lhes serviço mais rapidamente, agora que podem identificar os oportunistas em menos rodadas de simulação.

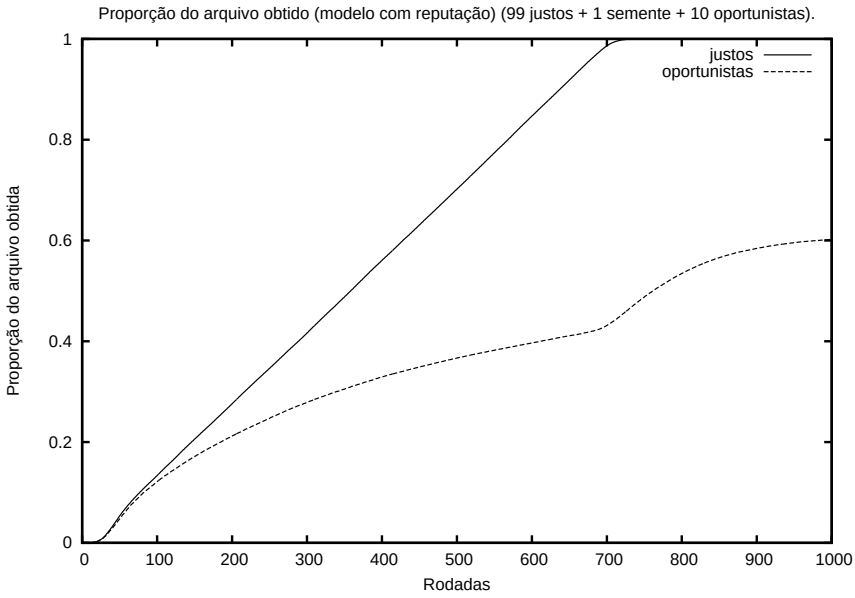


Figura 5.8: Proporção do arquivo obtido por justos e por oportunistas que não compartilham nada

Considerando esse novo modelo multiplicativo, é importante ver como ele reage a nós oportunistas simples. A Figura 5.8 apresenta a proporção do arquivo obtida por nós justos e oportunistas utilizando o modelo de reputação multiplicativo. podemos observar que, apesar do protocolo *BitTorrent* original conseguir bloquear mais oportunistas até o momento que ainda existem pares no sistema (permitindo cerca de 30% de downloads de oportunistas segundo a Figura 5.4 contra 40% do modelo com reputação), o modelo com reputação consegue conter mais os oportunistas após todos os pares se tornarem sementes, terminando a simulação com os oportunistas obtendo 60% do arquivo contra 70% no protocolo original.

5.5 Sumário

Este capítulo apresentou o protocolo *BitTorrent*, mostrando suas qualidades e seus problemas. Mostramos que o protocolo é capaz de disseminar um conteúdo sem sobrecarregar o fornecedor original do mesmo e que ele é bastante robusto para excluir nós oportunistas simples. Porém, quando os nós oportunistas utilizam uma estratégia um pouco mais complexa, aproveitando-se dos valores mínimos exigidos de serviço para

não serem considerados oportunistas, o protocolo *BitTorrent* passa a não apresentar um desempenho tão bom. Aplicamos, então, o modelo de reputações de Rocha a esse protocolo para obter melhores resultados na exclusão de oportunistas mais complexos, com resultados satisfatórios.

Capítulo 6

Conclusões e trabalhos futuros

Neste trabalho, apresentamos um estudo detalhado do comportamento do modelo baseado em reputação apresentado por Rocha [32]. Verificamos o impacto de alguns de seus parâmetros no desempenho do sistema e observamos que esse modelo apresenta bom desempenho na detecção e remoção de nós oportunistas em uma rede de roteamento sobreposta. Contudo, quando os nós oportunistas trabalham em conluio na tentativa de adulterar o estado da rede, o sistema como proposto é era capaz de reagir de forma adequada.

Dessa forma, propusemos algumas alterações ao modelo original para que ele possa reagir como esperado em meio a uma situação de conluio de nós oportunistas ou um ataque Sybil. Essas alterações têm como base um enriquecimento do critério para escolha de quais nós são confiáveis a ponto de se utilizar suas opiniões no cálculo da reputação. Observamos que essas modificações trouxeram melhorias ao desempenho do sistema em uma situação de ataque Sybil, ao mesmo tempo que não trouxe impacto negativo ao ambiente da proposta original, onde os nós oportunistas agiam sozinhos.

Também avaliamos o uso de protocolos de rumores para a manutenção do estado global exigido para o funcionamento do modelo baseado em reputação. Essa alteração é considerada importante, devido ao interesse em se utilizar o modelo em ambientes diferentes daquele para o qual ele foi desenvolvido. Nesses casos, a manutenção do estado global da forma como ocorria não permitia grande escalabilidade ao modelo. Aplicamos um protocolo de rumores alterado, tomando como base algumas da alterações utilizadas para combater ataques Sybil, que permitiu que o modelo continuasse a apresentar resistência a ataques de conluio e de nós oportunistas.

Finalmente, aplicamos o modelo de reputações a um ambiente diferente, o da rede de compartilhamento de arquivos *BitTorrent*, também para combater o comportamento oportunista, dessa vez no compartilhamento de arquivos. Vimos que, devido às diferenças inerentes às próprias aplicações (roteamento sobreposto e compartilhamento de

arquivos), o modelo teve de ser novamente alterado para apresentar o comportamento desejado. Como a identificação de comportamento oportunista em uma rede de compartilhamento de arquivos não é tão facilmente avaliado, tornou-se necessário alterar o modelo de forma que o decréscimo da experiência individual a cada experiência negativa fosse mais eficaz. Dessa forma, alteramos essa função para que ela utilize redução multiplicativa (tornando-se uma fração do valor atual), enquanto o acréscimo em caso de experiência positiva continua sendo feita de forma aditiva (somando-se um valor fixo). Verificamos que essas alterações melhoraram o desempenho na descoberta e exclusão de nós oportunistas ao mesmo tempo que não causou degradação sensível no serviço provido a nós justos.

6.1 Trabalhos futuros

Mesmo com as alterações propostas, o problema de *whitewashing* (nós oportunistas deixando a rede e retornando com uma identidade diferente, de forma a poder continuar usando o sistema de forma oportunista até ser excluído novamente) ainda existe. Esse problema persiste, pois não foi alterada a premissa que todos os nós recém chegados à rede são considerados "inocentes (justos) até que se prove o contrário".

Além disso, no Capítulo 5 nós alteramos a política de diminuição de experiência individual a cada interação mal sucedida para que que ela ocorresse de forma multiplicativa. Contudo, essa alteração foi aplicada apenas ao protocolo *BitTorrent*. Seria interessante avaliar o impacto que essa nova política teria nos ambientes apresentados nos capítulos anteriores.

Outro ponto interessante seria o estudo mais aprofundado do uso do modelo no protocolo *BitTorrent*, visto que nossos experimentos foram apenas preliminares para a avaliação se o protocolo poderia ser usado de forma adequado nesse novo contexto. Todavia, nosso simulador não compreende todos os detalhes do funcionamento de uma rede tão complexa, como congestionamento da rede, detalhes da manutenção de uma conexão TCP, entre outras.

Referências Bibliográficas

[1] A. Adya, W. Bolosky, M. Castro, R. Chaiken, G. Cermak, J. Douceur, J. Howell, J. Lorch, M. Theimer, and R. Wattenhofer. Farsite: Federated, available, and reliable storage for an incompletely trusted environment, 2002.

[2] David Andersen, Hari Balakrishnan, Frans Kaashoek, and Robert Morris. Resilient overlay networks. In *SOSP '01: Proceedings of the eighteenth ACM symposium on Operating systems principles*, pages 131–145, New York, NY, USA, 2001. ACM Press.

[3] Nazareno Andrade, Miranda Mowbray, Aliandro Lima, Gustavo Wagner, and Matei Ripeanu. Influences on cooperation in bittorrent communities. In *P2PECON '05: Proceeding of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pages 111–115, New York, NY, USA, 2005. ACM Press.

[4] David Arthur and Rina Panigrahy. Analyzing bittorrent and related peer-to-peer networks. In *SODA '06: Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 961–969, New York, NY, USA, 2006. ACM Press.

[5] Ashwin R. Bharambe, Cormac Herley, and Venkata N. Padmanabhan. Analyzing and improving bittorrent performance. Technical report, 2005.

[6] Ashwin R. Bharambe, Cormac Herley, and Venkata N. Padmanabhan. Some observations on bittorrent performance. In *SIGMETRICS '05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, pages 398–399, New York, NY, USA, 2005. ACM Press.

[7] S. Buchegger and J. Le Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes — fairness in dynamic ad-hoc networks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH*, June 2002.

[8] S. Buchegger and J. Le Boudec. Coping with false accusations in misbehavior reputation systems for mobile ad-hoc networks, 2003.

[9] S. Buchegger and J. Le Boudec. The effect of rumor spreading in reputation systems for mobile ad-hoc networks, 2003.

[10] Sonja Buchegger and Jean-Yves Le Boudec. A robust reputation system for p2p and mobile ad-hoc networks, 2004.

[11] Bram Cohen. Incentives to build robustness in bittorrent. In *http://bitconjurer.org/BitTorrent/bittorrentecon.pdf*, 2003.

[12] P. Costa, M. Migliavacca, G. P. Picco, and G. Cugola. Epidemic algorithms for reliable content-based publish-subscribe: An evaluation. In *Proc. of the 24rd Int. Conf. on Distributed Computing System s (ICDCS)*, pages 552–561, 2003.

[13] Frank Dabek, M. Frans Kaashoek, David Karger, Robert Morris, and Ion Stoica. Wide-area cooperative storage with CFS. In *Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP '01)*, Chateau Lake Louise, Banff, Canada, October 2001.

[14] George Danezis, Chris L. Laas, Frans M. Kaashoek, and Ross Anderson. Sybil-resistant dht routing. In *ESORICS*, pages 305–318, September 2005.

[15] A. Datta, S. Quarteroni, and K. Aberer. Autonomous gossiping: A self-organizing epidemic algorithm for selective information dissemination in mobile ad-hoc networks, 2004.

[16] Alan Demers, Dan Greene, Carl Houser, Wes Irish, John Larson, Scott Shenker, Howard Sturgis, Dan Swinehart, and Doug Terry. Epidemic algorithms for replicated database maintenance. *SIGOPS Oper. Syst. Rev.*, 22(1):8–32, 1988.

[17] Jochen Dinger and Hannes Hartenstein. Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. *ares*, 0:756–763, 2006.

[18] John R. Douceur. The sybil attack. In *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, London, UK, 2002. Springer-Verlag.

[19] Alex Fabrikant, Ankur Luthra, Elitza Maneva, and Christos H. Papadimitriou e Scott Shenker. On a network creation game. In *PODC '03: Proceedings of the*

twenty-second annual symposium on Principles of distributed computing, pages 347–351, New York, NY, USA, 2003. ACM Press.

[20] Michal Feldman and John Chuang. Overcoming free-riding behavior in peer-to-peer systems. *SIGecom Exch.*, 5(4):41–50, 2005.

[21] M. Izal, G. Urvoy-Keller, E. Biersack, P. Felber, A. Hamra, and L. Garces-Erice. Dissecting bittorrent: Five months in a torrent's lifetime, 2004.

[22] V. Jacobson. Congestion avoidance and control. *SIGCOMM Comput. Commun. Rev.*, 25(1):157–187, 1995.

[23] Seung Jun and Mustaque Ahamad. Incentives in bittorrent induce free riding. In *P2PECON '05: Proceeding of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pages 116–121, New York, NY, USA, 2005. ACM Press.

[24] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *WWW '03: Proceedings of the 12th international conference on World Wide Web*, pages 640–651, New York, NY, USA, 2003. ACM Press.

[25] David Kempe, Jon M. Kleinberg, and Alan J. Demers. Spatial gossip and resource location protocols. In *ACM Symposium on Theory of Computing*, pages 163–172, 2001.

[26] Nathaniel Leibowitz, Matei Ripeanu, and Adam Wierzbicki. Deconstructing the kazaa network. *wiapp*, 00:112, 2003.

[27] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the third international symposium on Information processing in sensor networks (IPSN-04)*, pages 259–268, New York, April 26–27 2004. ACM Press.

[28] Daniel Petrie. Sybil, 1976.

[29] J. Pouwelse, P. Garbacki, D. Epema, and H. Sips. A measurement study of the bittorrent peer-to-peer file-sharing system, 2004.

[30] Dongyu Qiu and R. Srikant. Modeling and performance analysis of bittorrent-like peer-to-peer networks. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 367–378, New York, NY, USA, 2004. ACM Press.

[31] M. Ripeanu. Peer-to-peer architecture case study: Gnutella network, 2001.

[32] B. G. Rocha, V. Almeida, and D. O Guedes. Increasing quality of service in selfish overlay networks. *IEEE Internet computing*, 10:24–31, 2006.

[33] Bruno Gusmão Rocha. Estratégias para aumentar a confiabilidade em redes sobrepostas com nós egoístas. Master's thesis, Universidade Federal de Minas Gerais (UFMG), Departamento de Ciência da Computação, October 2005.

[34] B. Prabhakar S. Boyd, A. Ghosh and D. Shah. Gossip algorithms: Design, analysis and applications. In *Proc. IEEE Infocom 2005 Volume 3*, pages 1653–1664, March 2005.

[35] D. Sivakumar S. Gollapudi and A. Zhang. Exploiting anarchy in networks: A game-theoretic approach to combining fairness and throughput, March 2005.

[36] Flora Rheta Schreiber. *Sybil*. Warner Books, 1973.

[37] Jean-Marc Seigneur, Alan Gray, and Christian Damsgaard Jensen. Trust transfer: Encouraging self-recommendations without sybil attack. In *iTrust*, pages 321–337, 2005.

[38] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 149–160, New York, NY, USA, 2001. ACM Press.

[39] Kevin Walsh and Emin Gün Sirer. Experience with a distributed object reputation system for peer-to-peer filesharing. In *NSDI '06: Proceedings of the Symposium on Networked System Design and Implementation*, 2006.

Apêndice A

Apêndice: Gráficos com Desvio Padrão

A.1 O ataque Sybil

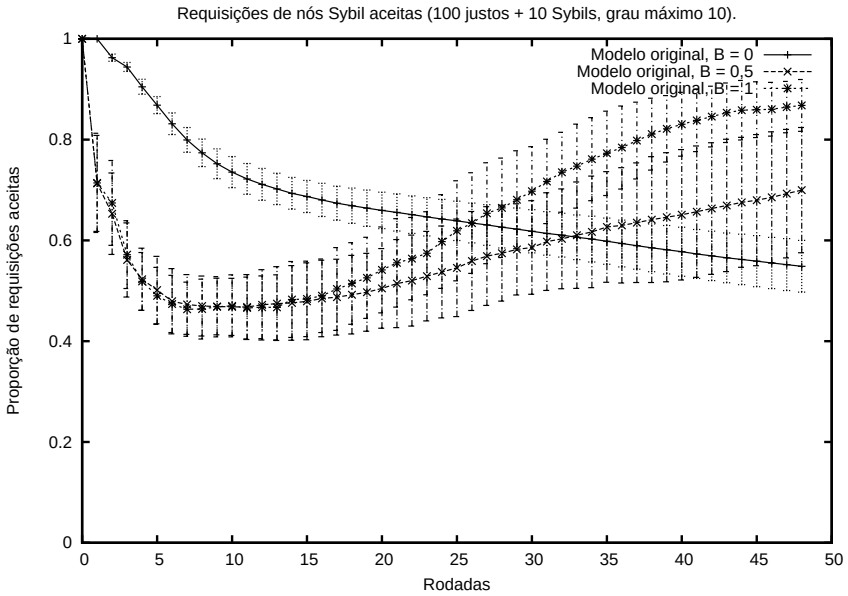


Figura A.1: Requisições de nós Sybil aceitas no modelo original (com desvio padrão, referente à Figura 3.1)

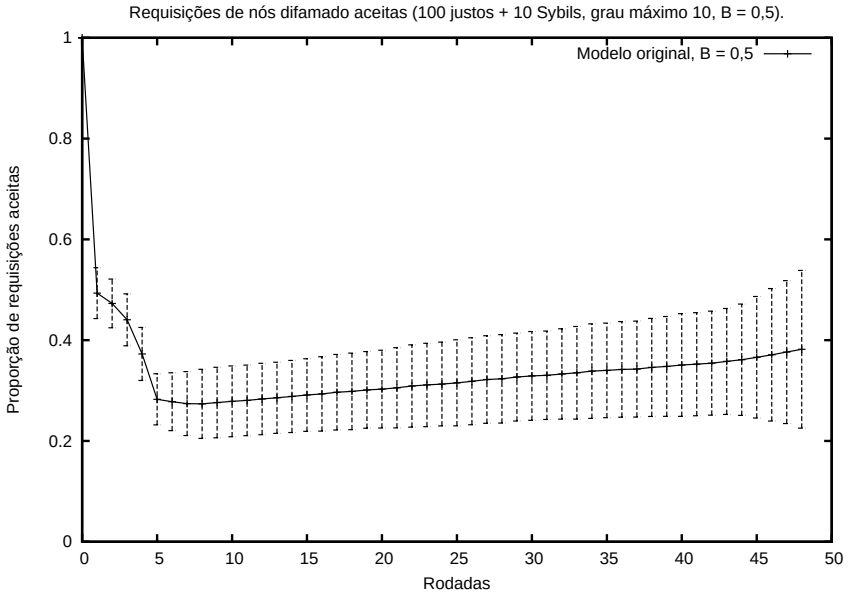


Figura A.2: Requisições de um nó justo aceitas quando nós Sybil em conluio tentam difamá-lo (com desvio padrão, referente à Figura 3.2)

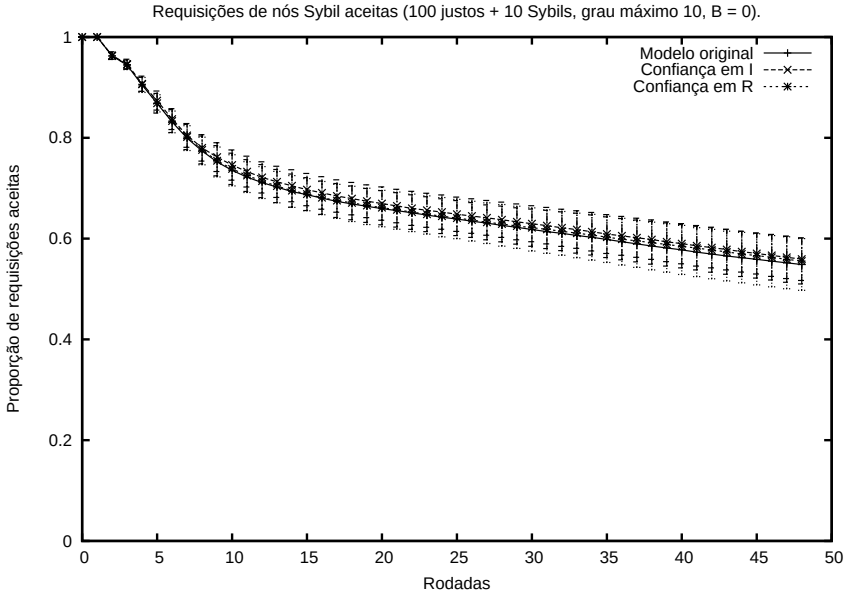


Figura A.3: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0$ (com desvio padrão, referente à Figura 3.3)

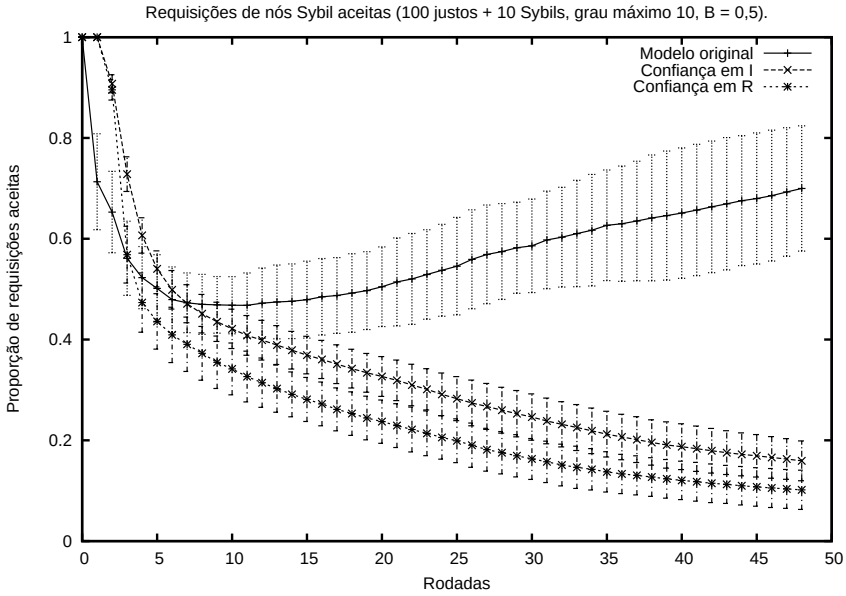


Figura A.4: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$ (com desvio padrão, referente à Figura 3.4)

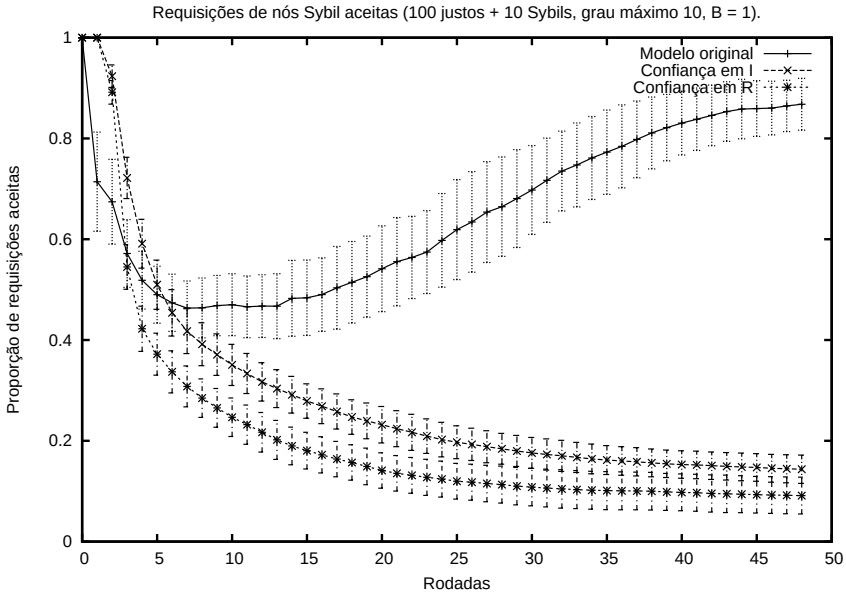


Figura A.5: Requisições de nós Sybil aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 1$ (com desvio padrão, referente à Figura 3.5)

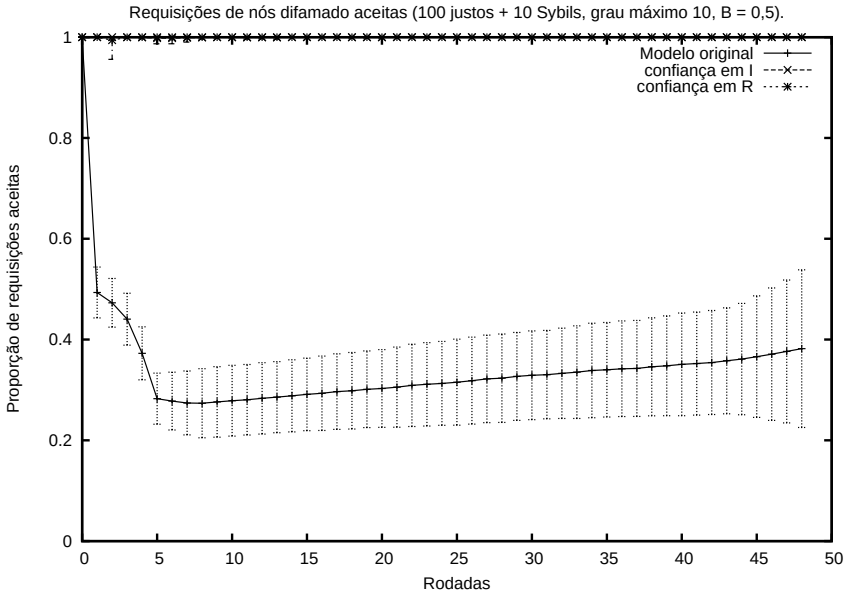


Figura A.6: Requisições de um nó difamado por Sybils aceitas nos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$ (com desvio padrão, referente à Figura 3.6)

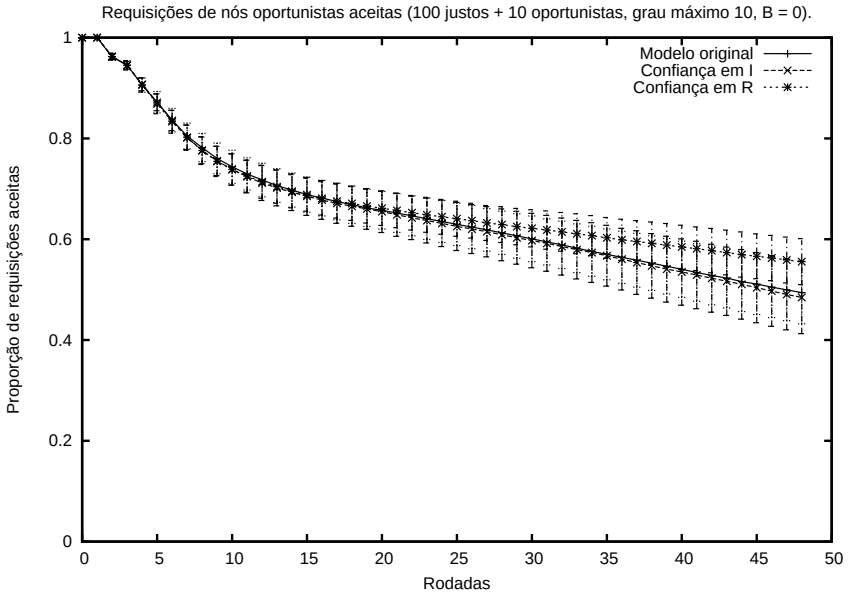


Figura A.7: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0$ (com desvio padrão, referente à Figura 3.8)

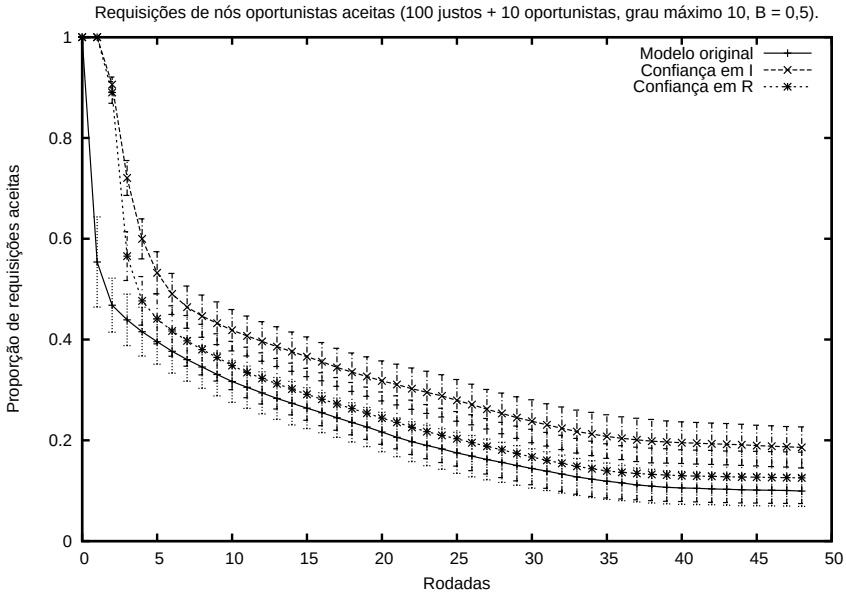


Figura A.8: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 0,5$ (com desvio padrão, referente à Figura 3.9)

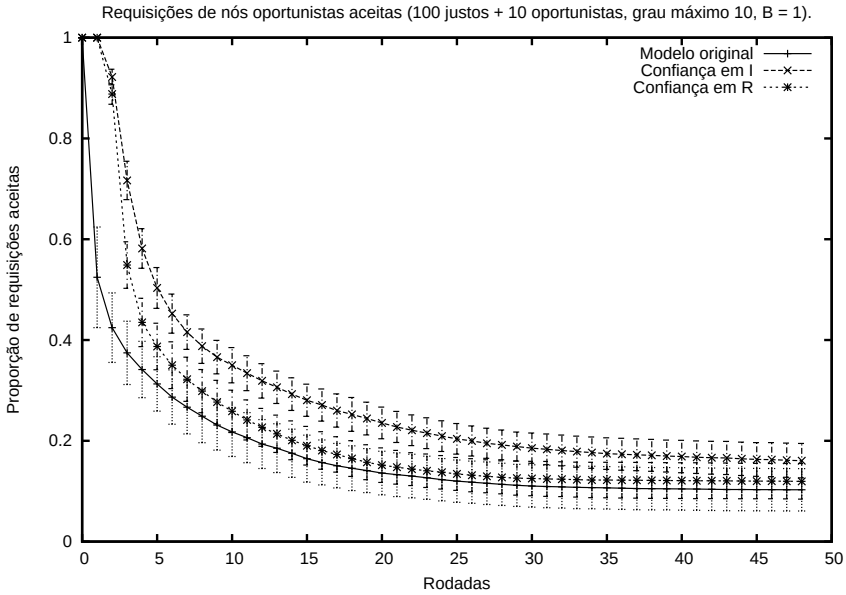


Figura A.9: Requisições de nós oportunistas aceitas pelos modelos original e com confiança baseada na experiência individual e na reputação para $\beta = 1$ (com desvio padrão, referente à Figura 3.10)

A.2 Protocolos de rumores

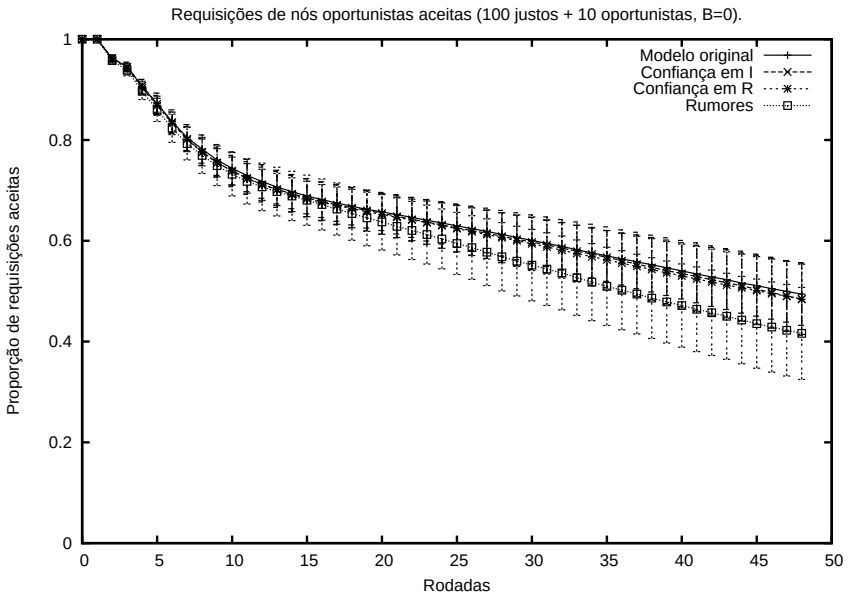


Figura A.10: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 0$ (com desvio padrão, referente à Figura 4.6)

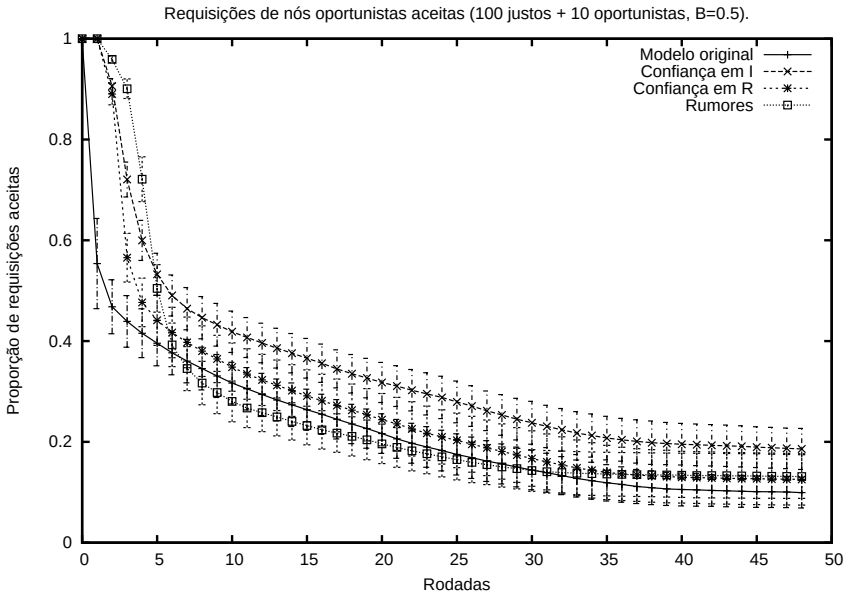


Figura A.11: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 0,5$ (com desvio padrão, referente à Figura 4.7)

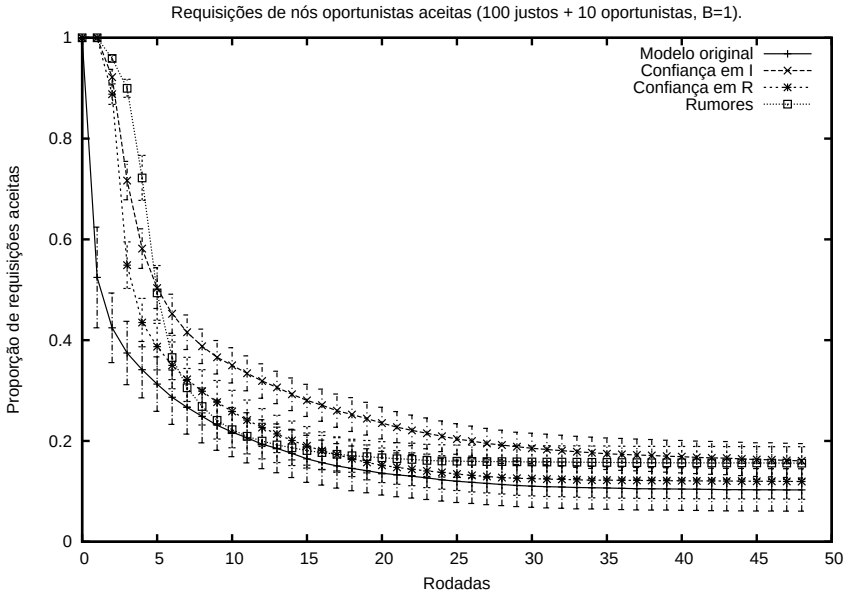


Figura A.12: Serviço fornecido a nós oportunistas com modelos que usam conhecimento global e com modelo de rumores com $\beta = 1$ (com desvio padrão, referente à Figura 4.8)

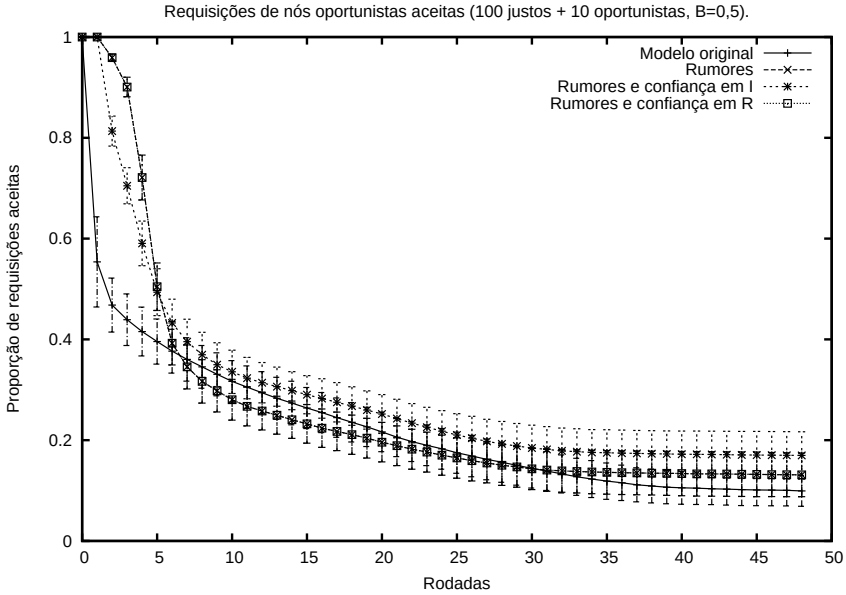


Figura A.13: Serviço fornecido a nós oportunistas com modelo de rumores simples e rumor utilizando confiança na experiência individual e reputação com $\beta = 0,5$ (com desvio padrão, referente à Figura 4.9)

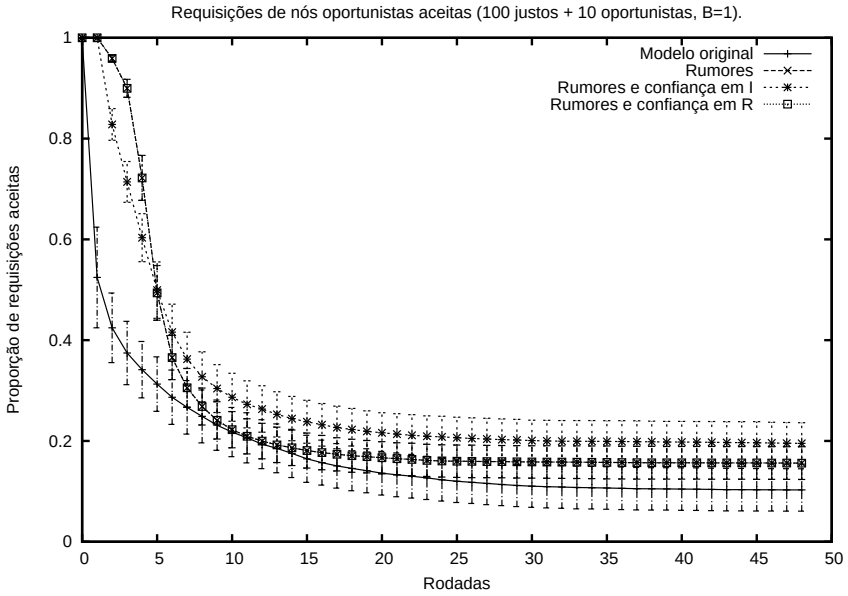


Figura A.14: Serviço fornecido a nós oportunistas com modelo de rumores simples e rumor utilizando confiança na experiência individual e reputação com $\beta = 1$ (com desvio padrão, referente à Figura 4.10)

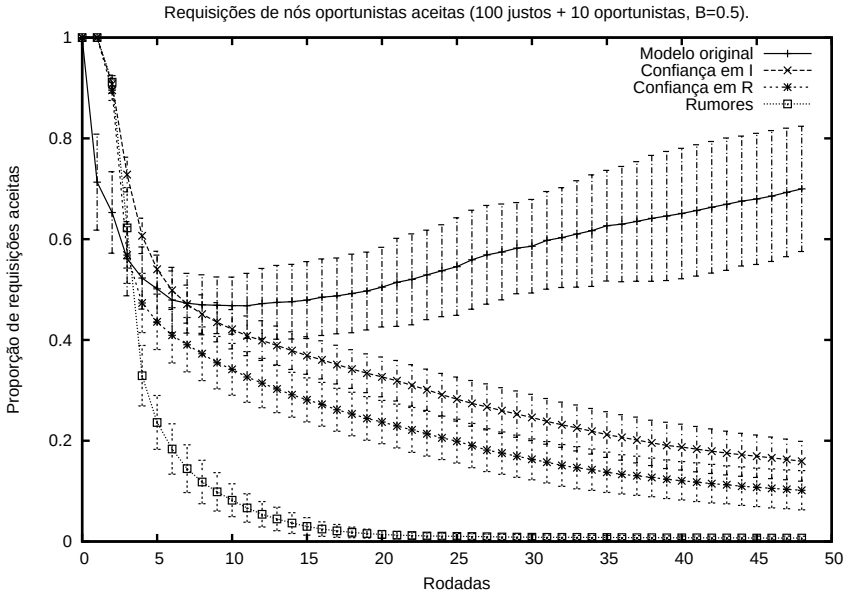


Figura A.15: Serviço fornecido a nós Sybil no modelo original e no modelo com rumores para $\beta = 0,5$ (com desvio padrão, referente à Figura 4.11)

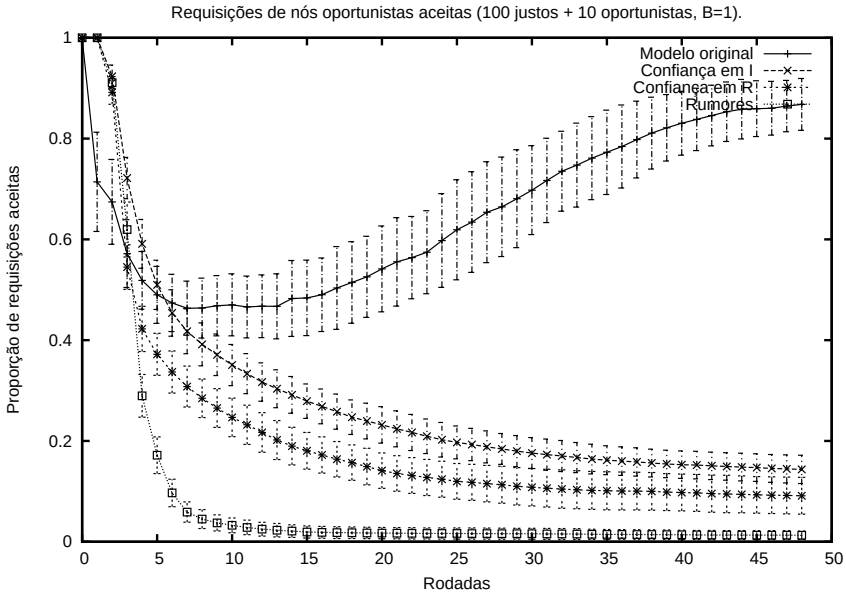


Figura A.16: Serviço fornecido a nós Sybil no modelo original e no modelo com rumores para $\beta = 1$ (com desvio padrão, referente à Figura 4.12)

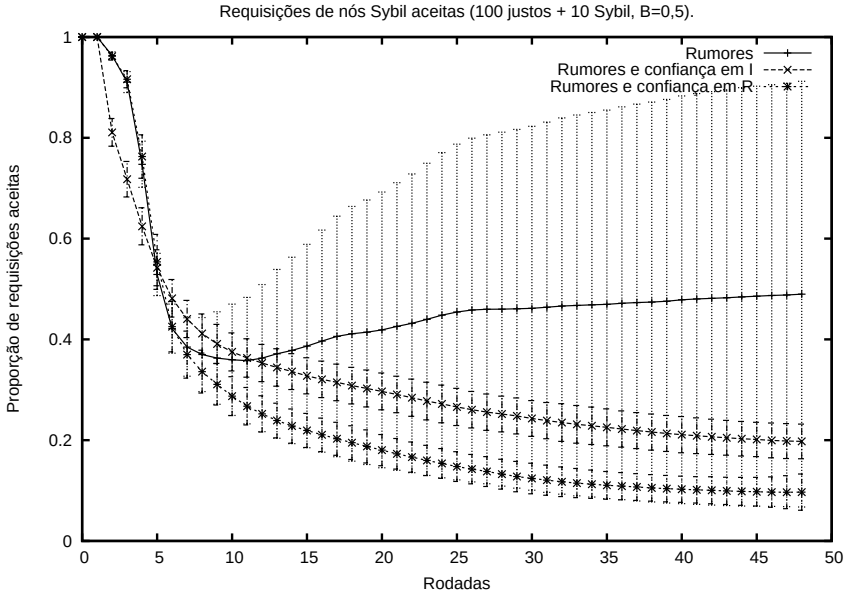


Figura A.17: Serviço fornecido a nós Sybil com modelo de rumores simples e rumores com confiança na experiência individual e na reputação, com $\beta = 0,5$ e Sybils aceitando até 10% das requisições (com desvio padrão, referente à Figura 4.13)

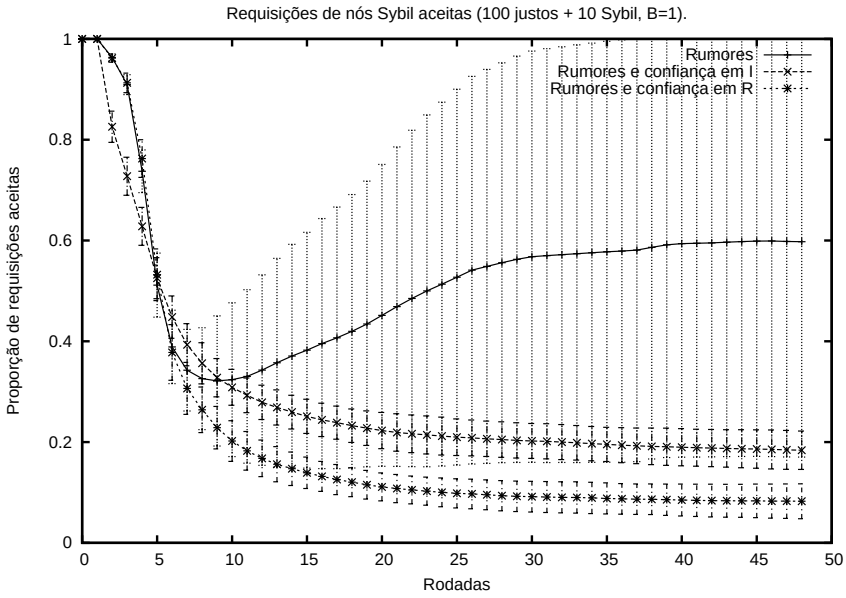


Figura A.18: Serviço fornecido a nós Sybil com modelo de rumores simples e rumores com confiança na experiência individual e na reputação, com $\beta = 1$ e Sybils aceitando até 10% das requisições (com desvio padrão, referente à Figura 4.14)

A.3 A rede BitTorrent

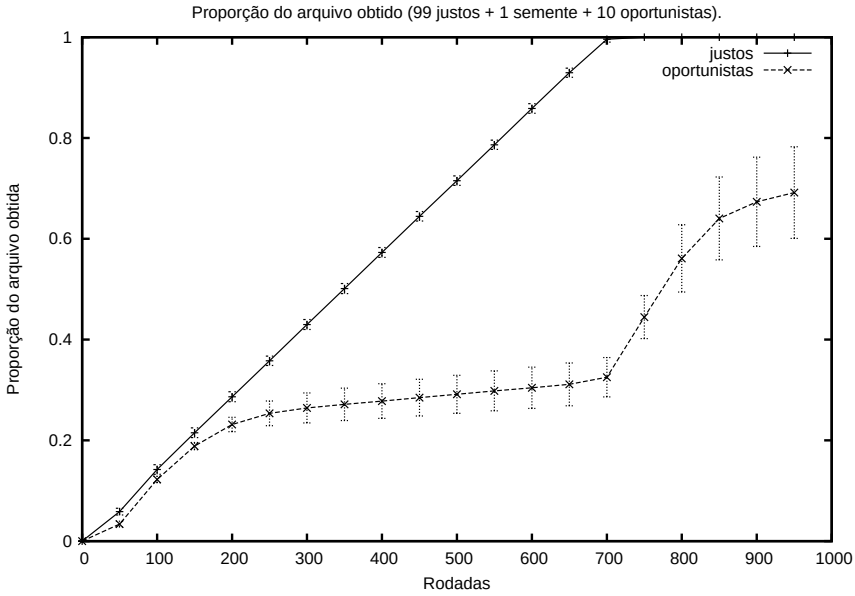


Figura A.19: Proporção do arquivo obtido por oportunistas e justos numa rede *BitTorrent* tradicional (com desvio padrão, referente à Figura 5.4)

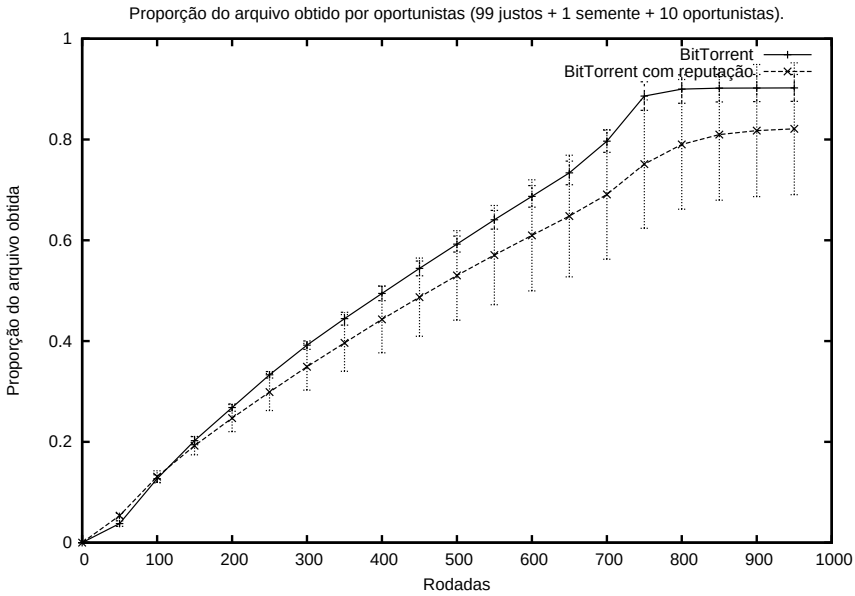


Figura A.20: Proporção do arquivo obtido por oportunistas que compartilham o mínimo possível 10% do tempo para o BitTorrent tradicional e com reputação (com desvio padrão, referente à Figura 5.6)

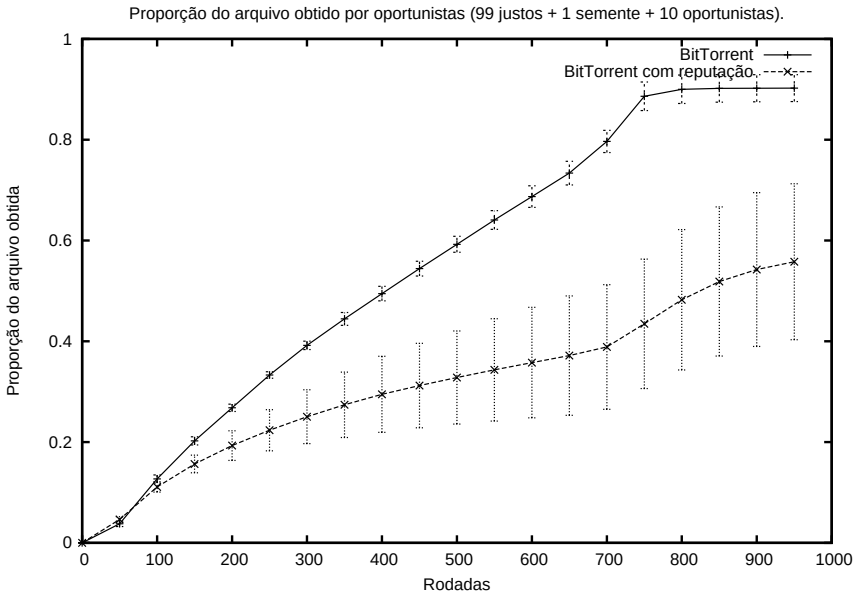


Figura A.21: Proporção do arquivo obtido por oportunistas que compartilham o mínimo possível 10% do tempo para o BitTorrent tradicional e com reputação com $\gamma = 0,75$ (com desvio padrão, referente à Figura 5.7)