Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estratégias para Aumentar a Confiabilidade em Redes Sobrepostas com Nós Egoístas

Bruno Gusmão Rocha

Dissertação de Mestrado apresentada ao Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.
Orientador: Virgílio A. F. Almeida
Co-Orientador: Dorgival Olavo Guedes

Belo Horizonte
Outubro de 2005

Agradecimentos

Inicialmente, eu gostaria de agradecer ao DCC/UFMG pelo apoio e pelas oportunidades concedidos durante o mestrado e a graduação. Aos meus orientadores, Vírgilio e Dorgival, que tanto contribuíram com idéias, atenção, trabalho, e que sempre fizeram as perguntas que eu precisava ouvir, me estimulando a continuar fazendo essas mesmas perguntas pelo resto da vida.

Ao professor Wagner Meira, que me orientou durante toda a graduação e com quem aprendi muito mais do que apenas como fazer pesquisa.

Ao pessoal da Telemig, pela compreensão e por pintar com alegria o meu dia-a-dia. Em especial, gostaria de agradecer ao Ronaldo, por ter permitido a flexibilização do meu horário, sem a qual eu não teria conseguido cumprir os créditos das disciplinas.

Aos meus pais, que fizeram tudo isso possível, devo tudo a vocês! A minha parte nessa conquista é bem menor que a de vocês, e será assim em todas as outras irão por vir. Aos meus irmãos, Lúcio, Thiago e Rafael pelo apoio, e a todos os meus familiares que torceram por mim.

Aos meus amigos, por gozarem dos meus maiores problemas, tirar-me de casa quando eu não podia e convencer-me a gastar meu tempo com algum jogo online ao invés de trabalhar na minha tese. Sem vocês, eu teria terminado o mestrado mais rápido, mas a vida não teria sido tão divertida.

A Olga, pela presença constante, o companheirismo e a leveza que distribui onde estiver.

A Deus, por iluminar o meu caminho, e ter-me dado tanto, quando tantos tem tão pouco.

Resumo

Recentemente, o surgimento de um novo paradigma de redes tornou possível o desenvolvimento de aplicações nos mais variados domínios. Trata-se das *Redes de Roteamento Sobrepostas*. As redes de roteamento sobrepostas utilizam a atual infra-estrutura da Internet para prover suporte à aplicações tão diversas quanto garantia de qualidade serviço (QoS), multicast, busca, etc. O sucesso de tais sistemas é baseado na premissa de que todos os participantes da rede estão dispostos a cooperar mutuamente, e disponibilizar seus próprios recursos para os seus pares. Entretanto, na prática torna-se provável que os nós agirão racionalmente e de uma forma egoísta. Por racional, entende-se que os nós nunca tomarão ações que possam impactar negativamente seus próprios interesses, e por egoísta, implica-se que os nós buscarão satisfazer apenas seus objetivos ao utilizar a rede, sem se importar com o bem global.

Dessa maneira, os nós tenderiam a ignorar qualquer protocolo ou política pré-definidos que não levassem seus objetivos individuais em consideração. Esses nós egoístas são compelidos a explorar ao máximo os recursos da rede, e ao mesmo tempo, prover a menor quantidade possível de seus próprios recursos em troca. Mais ainda, os nós podem ser tentados a negar completamente o acesso a seus recursos se não houver nenhum incentivo contra essa estratégia, já que isso representaria um custo zero de participação na rede. Claramente, tal comportamento representa um impacto na *confiabilidade* do serviço provido pela rede sobreposta, já que haverá menos participantes contribuindo em relação àqueles que utilizam os recursos. De fato, se muitos nós decidirem adotar esse comportamento oportunista (*free-rider behavior*), toda a rede pode eventualmente entrar em colapso.

Nessa dissertação, buscamos abordar o problema do aumento da confiabilidade em redes sobrepostas através da detecção e exclusão de nós oportunistas. Introduzimos nessas redes o conceito de *reputação*, que é uma medida de da confiabilidade e justiça de um nó em relação a seus pares. Nós com

altas reputações tem uma grande chance de terem as suas requisições atendidas na rede, e podem inclusive ter essas requisições priorizadas sobre aquelas de nós com reputações mais baixas. Por outro lado, nós com baixas reputações possuem uma alta probabilidade de terem seus pedidos negados, já que poucos membros da rede sobreposta estariam dispostos a prover serviços a um nó que provavelmente não retribuiria no futuro o uso dos recursos dispensados. Dessa maneira, torna-se interessante para todos os nós, mesmo os egoístas, alcançar e manter a melhor reputação possível. O mecanismo aqui proposto explora a natureza intrinsicamente egoísta e racional dos nós para direcionar seu comportamento à confiabilidade, condição necessária para se obter uma alta reputação na rede.

Conduzimos nosso estudo modelando a formação da rede como um jogo não-cooperativo, no qual os jogadores estabelecem conexões com seus vizinhos buscando maximizar seus próprios benefícios, isto é, escolhendo os vizinhos com a menor latência e a mais alta reputação possível. O resultado desse jogo é a topologia da rede dada pelo *Equilíbrio de Nash*. O equilíbrio de Nash é uma noção fundamental na teoria dos jogos, e é caracterizado pelo conjunto de estratégias adotadas por cada jogador tal que não há nenhum incentivo para alterar a estratégia adotada enquanto todos os outros jogadores mantém suas estratégias. Nosso objetivo ao modelar o mecanismo é definir as regras básicas para este jogo não-cooperativo, de forma que a confiabilidade é aumentada e os nós oportunistas são virtualmente excluídos no equilíbrio de Nash.

Nosso mecanismo admite uma implementação distribuída, descentralizada e assíncrona. Demonstramos através de uma série de experimentos as propriedades das topologias obtidas e a eficiência na exclusão dos nós oportunistas, e mostramos como a utilização de tal mecanismo pode aumentar significamente a justiça e a confiabilidade nas redes sobrepostas.

Sumário

Agradecimentos iii
Resumo v
Sumário viii
Lista de Figuras ix
Lista de Tabelas 1

1 Introdução **3**
1.1 Redes Sobrepostas 3
1.1.1 Redes de Roteamento Sobrepostas 4
1.1.2 Redes Sobrepostas Egoístas 4
1.1.3 Nós Oportunistas 5
1.2 Motivação 5
1.3 Contribuição 6
1.4 Organização do Trabalho 6

2 Trabalhos Relacionados **9**
2.1 Redes Sobrepostas Egoístas 9
2.2 Justiça e Confiabilidade em Redes Sobrepostas Egoístas 10
2.2.1 Mecanismos Baseados em Valores 10
2.2.2 Mecanismos Baseados em Reputação 11
2.2.3 Mecanismos Baseados em Jogos Estratégicos 11

3 Modelo Proposto **13**
3.1 Formulação do Problema 13
3.2 Estratégias Baseadas em Reputação 15
3.2.1 Experiência Individual 15
3.2.2 Reputação 17
3.3 Uma Abordagem Baseada em Teoria dos Jogos 18
3.3.1 Função de Utilidade 19
3.3.2 Modelo do Jogo 20

4 Avaliação Experimental **25**
4.1 Métricas 26
4.2 Estratégias Avaliadas 27
4.3 Avaliação Experimental 27

5 Conclusão e Trabalhos Futuros **35**
5.1 Conclusões 35
5.2 Trabalhos Futuros 35

Referências **39**

Lista de Figuras

3.1 Redes Sobrepostas Egoístas 14

4.1 Requisições aceitas variando-se α 28
4.2 Serviço provido aos nós oportunistas 29
4.3 Serviço provido aos nós justos 29
4.4 Nós Alcançáveis 30
4.5 Amostra de topologia gerada pela estratégia gulosa (nós oportunistas em preto) 31
4.6 Amostra de topologia gerada pela estratégia baseada em reputação (nós oportunistas em preto) 32
4.7 Índice de Confiabilidade 33
4.8 Número médio de partições na rede sobreposta 33

Lista de Tabelas

4.1 Estratégias avaliadas com suas respectivas funções de utilidade . 27

CAPÍTULO 1

Introdução

Este capítulo tem por objetivo apresentar a área de redes de roteamento sobrepostas, e algumas de suas implicações e desafios. Primeiramente, será feita uma descrição das características e dos principais componentes dessas redes. Em seguida, serão apresentadas algumas áreas de aplicação em que essas redes podem vir a atuar. O assunto será concluído com uma análise dos principais problemas encontradas nessa emergente área de pesquisa. Ainda apresentamos brevemente o problema tratado nesta dissertação, juntamente com a sua motivação. Para concluir, a organização do texto, como um todo, será resumida no final deste capítulo.

1.1 Redes Sobrepostas

As redes de computadores vêm se mostrando ao longo das últimas décadas um dos mais excitantes e férteis campos de pesquisa na Ciência da Computação. A evolução de tais redes levou ao surgimento da *Internet*, composta por milhares de redes de computadores comerciais, acadêmicas, domésticas e governamentais de menor escala. A Internet possibilita a comunicação e a transferência de dados e informações entre as redes menores que a compõe.

Muitos sistemas utilizam a infra-estrutura provida pela Internet para montar uma rede lógica a nível de aplicação. Um exemplo simples desse tipo de abordagem são as redes par-a-par (*peer-to-peer networks*), muito utilizadas por sistemas de compartilhamento de arquivos, como o BitTorrent [7], Kazaa [20] e Gnutella [23]. Muitos outros serviços podem ser facilmente desenvolvidos e implementados usando o princípio de redes sobrepostas, já que essa técnica permite uma dependência menor do suporte da rede substrato. Em outras

palavras, serviços sobrepostos incluindo o desenvolvimento de novas aplicações e protocolos podem utilizar efetivamente a abordagem de sobreposição, já que através desta não há nenhuma requisição de mudanças nas camadas inferiores de rede.

Uma rede sobreposta é formada por um subconjunto de nós físicos subjacentes. As conexões entre os nós sobrepostos são providas por elos sobrepostos (caminhos na camada IP), que usualmente são compostos por uma ou mais conexão física. Como as aplicações sobrepostas são construídas na camada de aplicação, elas podem efetivamente utilizar a Internet como uma infra-estrutura em um nível mais baixo para prover serviços de mais alto nível aos usuários finais.

1.1.1 Redes de Roteamento Sobrepostas

Embora atualmente exista um grande número de aplicações potenciais que poderiam se beneficiar da arquitetura de redes sobrepostas, com a possível exceção dos sistemas de compartilhamento de arquivo, ainda não há redes de grande porte utilizando esta tecnologia, embora existam inúmeros protótipos. Dentre os vários serviços e aplicações propostas, podemos destacar garantia de qualidade de serviço [19], multicast [18], busca [28], armazenamento global e compartilhamento [25] e redes de roteamento [1, 26]. Destas, um das mais promissoras aplicações são as redes de roteamento sobrepostas, que podem servir de base para uma miríade de serviços e tecnologias.

As *Redes de Roteamento Sobrepostas* (Routing Overlay Networks - RON) são particularmente efetivas em contornar falhas, períodos de congestionamento e desempenho degradado na rede. Enquanto as RON provém períodos de recuperação de apenas alguns segundos, os atuais protocolos de roteamento podem levar vários minutos para atingir a convergência. Os nós de um RON monitoram a qualidade dos caminhos e rotas da rede substrato (Internet) entre eles, e usam esta informação para decidir quando rotear pacotes diretamente pela Internet ou através de outros nós na RON, otimizando assim o desempenho das aplicações que executam na camada superior a eles. As RONs serão o enfoque do nosso estudo.

1.1.2 Redes Sobrepostas Egoístas

Um dos pressupostos básicos para o sucesso das redes de roteamento sobrepostas é que todos os nós estão dispostos a cooperar mutuamente entre si, liberando os recursos para seus pares esperando a reciprocidade por parte deles quando necessário. Entretanto, em situações realistas, é esperado que os nós sejam *racionais* e *egoístas*. Por racionais, entende-se que os nós nunca

tomam nenhuma ação contra seus próprios objetivos, e por egoístas, entende-se que eles buscam apenas satisfazer seus interesses particulares, sem se importar com o bem global.

Com isso, as ações dos nós não visam de forma alguma alcançar o "bem comum" na rede, pois sua única motivação é alcançar seus objetivos individuais. Tal comportamento pode inclusive ir contra a configurações que tragam o maior benefício global para todos os participantes.

1.1.3 Nós Oportunistas

Em uma rede sobreposta egoísta, são os protocolos e políticas definidos que devem tentar guiar as ações dos nós em direção ao ótimo global. Entretanto, tais nós podem vir a ignorar esses protocolos e políticas se esses forem diretamente contra seus interesses, devido a sua já citada natureza racional e egoísta. De fato, para aumentar seus benefícios na participação da rede, um nó egoísta tentaria fornecer a menor quantidade de recursos possíveis de forma a sempre tê-los disponíveis para si próprio, enquanto utilizando ao máximo os serviços providos pela rede. Em seu extremo, esse comportamento pode levar um participante da rede sobreposta a se negar completamente a servir as requisições dos seus pares, se não houver incentivos contra essa estratégia. Esses nós se tornariam então *nós oportunistas* (ou *free-riders*), parasitas da rede sobreposta, que apenas sugam seus recursos sem nunca retornar nada em troca. Obviamente, tal comportamento possui um impacto claro na qualidade de serviço provida pela rede, já que haveria mais consumidores para um menor número de fornecedores de serviços e recursos. No limite, o número de *free-riders* poderia crescer tanto que inviabilizaria a existência da rede.

1.2 Motivação

O objetivo desse trabalho é explorar o problema de aumento de confiabilidade em redes sobrepostas egoístas, através da detecção e exclusão de nós oportunistas.

Utilizamos uma abordagem orientada pela teoria dos jogos, onde modelamos a formação da rede sobreposta como um jogo não-cooperativo, em que os nós buscam estabelecer conexões com seus vizinhos de forma a maximizar seus benefícios (escolhendo conexões com a menor latência, por exemplo). O resultado desse jogo é a topologia da rede sobreposta dada pelo *equilíbrio de Nash*, uma noção fundamental na teoria dos jogos. O equilíbrio de Nash é caracterizado pelo conjunto de estratégias adotados por cada jogador, de forma que não existem incentivos para um jogador modificar sua estratégia enquanto

todos os outros jogadores mantém as suas próprias estratégias inalteradas.

Para tal, propomos um mecanismo baseado no conceito de *reputação* [2], que é definida em nosso modelo como uma medida justiça e confiabilidade de um nó na visão dos seus pares e das próprias interações entre cada nó. Nós com altas reputações tem uma grande chance de terem todas as suas requisições atendidas na rede, e mesmo de ter essas requisições priorizadas em relação àquelas de nós com reputações inferiores. Por outro lado, nós com baixas reputações possuem uma grande probabilidade de terem seus pedidos negados pelos participantes da rede sobreposta, já que poucos nós estariam dispostos a fornecer seus recursos para outros nós que não retribuiriam reciprocamente esses recursos quando necessário. Dessa maneira, é de interesse de todos os nós, inclusive dos egoístas e oportunistas, manter a mais alta reputação possível.

1.3 Contribuição

As principais contribuições apresentadas nessa tese são:

- Proposição de um mecanismo simples e eficaz para proteger a rede sobreposta dos nós oportunistas, impondo penalidades sobre tais nós e premiando aqueles que se comportam de maneira justa.
- Introdução das regras básicas que guiam o jogo não-cooperativo entre os nós, de forma a atingir uma topologia onde os nós egoístas sejam virtualmente excluídos da rede.
- Apresentação de um arcabouço de reputações, que são usadas para guiar as interações entre os nós. A determinação das reputações é feita de maneira simples, distribuída e flexível.
- Proposição de algoritmos que exploram a natureza intrinsicamente egoísta dos nós para direcionar seu comportamento a justiça, condição primordial para se obter e manter uma alta reputação na rede, e conseqüentemente, ter amplo acesso a seus serviços.

1.4 Organização do Trabalho

O texto desta dissertação é organizado da seguinte maneira. No Capítulo 2 serão apresentados os trabalhos relacionados ao problema aqui abordado. No Capítulo 3 será definido o problema abordado neste trabalho e feito um levantamento dos sub-problemas envolvidos. Além disso, também descrevemos a solução proposta e sua implementação. No Capítulo 4 serão apresentados

os resultados experimentais obtidos. E, finalmente, no Capítulo 5 será feita uma análise do trabalho realizado, apresentadas as principais conclusões do estudo e direções para trabalhos futuros.

CAPÍTULO 2

Trabalhos Relacionados

Neste capítulo serão discutidos os trabalhos relacionados ao problema de aumento de confiabilidade em redes sobrepostas egoístas. Primeiramente, descreveremos os trabalhos que analisam a natureza egoísta dos nós, e como eles usam uma abordagem baseada em Teoria dos Jogos para obter e analisar as redes formadas. Em seguida, descreveremos os mecanismos propostos na literatura que tentam contornar o problema de nós oportunistas e os comparamos à abordagem aqui apresentada.

2.1 Redes Sobrepostas Egoístas

O estudo das redes de roteamento sobrepostas tem recebido considerável atenção recentemente [1, 25, 28, 31]. Todas esses protocolos visam construir uma infra-estrutura de roteamento na camada de aplicação, que permite a rápida recuperação em períodos de falhas, congestionamento, ataques, etc. Como as decisões sobre o roteamento passam a ser tomadas para otimizar métricas individuais dos nós ao invés de levar em conta critérios que cobrem todo o sistema(como no roteamento tradicional), tais abordagens levam a uma rede sobreposta *egoísta*.

A caracterização das redes de roteamento sobrepostas com nós egoístas foi primeiramente mencionada por Feigenbaum e Shenker em [11]. Uma abordagem baseada em Teoria dos Jogos para o problema de criação de tais redes foi introduzida em [10]. O seu modelo, simplificado para possibilitar uma análise matemática do problema, estabelece que o custo de criação de uma aresta no grafo da rede é o mesmo para todos os nós, e que a distância entre dois nós é o número de *hops*. Nesse trabalho, é investigado o preço da anar-

quia, um conceito introduzido por Papadimitriou [22] que mostra a razão entre o pior caso no equilíbrio de Nash e o ótimo social, ou em outras palavras, o preço que os participantes pagam como um grupo por serem egoístas. Feigenbaum e Shenker provam limites superiores e inferiores para esta razão, e conjeturam que se o custo relativo de se estabelecer nós é alto o suficiente, todos os equilíbrios de Nash do jogo levam a árvores.

Em [24], os mesmos preceitos de Teoria dos Jogos são utilizados no estudo de redes egoístas, mas a latência é escolhida como métrica de desempenho. Nesse artigo, foi provado que o preço da anarquia pode depender da inclinação das funções de latência usadas. Embora o preço da anarquia possa ser alto no pior caso do equilíbrio de Nash, alguns estudos teóricos demonstraram que a degradação pode ser menos severa sob outras perspectivas. Por exemplo, Friedman mostrou que para a maioria dos vetores de tráfego em uma escala dada, o preço da anarquia é menor que o do pior caso [13]. Ele também analisou o efeito das taxas de adaptação do TCP em uma conexão paralela de rede e demonstrou que as perdas são limitadas.

A formação das topologias de rede sobrepostas por redes egoístas foi investigada em [6]. Vários cenários são explorados, mas todos têm em comum a premissa de que os nós participam de um jogo competitivo e não-cooperativo. As topologias finais são obtidas quando o jogo alcança o equilíbrio de Nash, e várias propriedades dessas topologias são dissecadas, como a resistência a falhas e a ataques, o desempenho e a conectividade dos nós.

2.2 Justiça e Confiabilidade em Redes Sobrepostas Egoístas

A questão de alocação justa de recursos em redes sobrepostas caracterizadas por ambientes competitivos e nós egoístas foi o foco de atenção de vários estudos.

2.2.1 Mecanismos Baseados em Valores

Uma abordagem comum para aumentar a confiabilidade da rede é a implementação de uma estrutura de preços no jogo, através da qual os jogadores podem fazer ofertas por *unidades de recursos*, tais como QoS [27], compartilhamento de arquivos [15] ou alocação de banda [30]. A implementação de tal mecanismo é variável, mas em geral pode ser divido em arquiteturas que fazem uso de uma entidade central para coordenar o processo [27, 15] ou distribuindo esta responsabilidade para os próprios jogadores [30], o que é mais condizente com o cenário das redes sobrepostas. Independentemente da

implementação escolhida, há uma premissa comum de que justiça e confiabilidade serão obtidas através da atribuição de valores aos recursos da rede, e a criação de um mercado onde os jogadores podem pagar e receber por seus serviços.

Embora uma idéia interessante, essa abordagem possui a desvantagem de requerer a implementação de um sistema de micro-pagamentos que possa permitir aos nós concluir suas transações, introduzindo assim uma complexidade extra desnecessária ao sistema. Além disso, o próprio sistema de micro-pagamentos ainda é um tópico de pesquisa em desenvolvimento [8, 29]. Mais ainda, há uma premissa comum de que os nós sobrepostos estariam dispostos a operar baseados em um arcabouço de preços, com um sistema de cobrança monetária explícita. Em contraste, muitas das mais bem sucedidas redes cooperativas hoje em dia usam mesma unidade (como largura de banda tornada disponível) tanto para recompensar quanto para taxar os participantes do sistema, em conjunto com a implementação de algum tipo de política de justiça [7]. Este é a abordagem que adotamos nesse trabalho.

2.2.2 Mecanismos Baseados em Reputação

Embora não diretamente voltadas para redes sobrepostas, outras abordagens também se ocuparam do problema de justiça em redes cooperativas.

O conceito de reputação foi usado no protocolo CONFIDANT [3], que computa a qualidade e confiabilidade dos serviços providos pelas nós em uma rede ad-hoc e decide a partir dessa informação qual será o caminho usado pelos pacotes enviados. O protocolo necessita de uma *lista de amigos*, para a qual seriam divulgadas as informações sobre as interações com os outros nós, mas a criação inicial de tal lista em um ambiente competitivo onde todos os nós são desconhecidos é um problema em aberto. Além disso, o protocolo não apresenta uma boa escalabilidade e nem é efetivo em lidar com *difamação*, onde um nó justo é maliciosamente relatado como oportunista.

2.2.3 Mecanismos Baseados em Jogos Estratégicos

As abordagens baseadas em jogos estratégicos utilizam algumas premissas formais para definir modelos onde os nós competem entre si, e a partir desse ponto chegar em uma situação de equilíbrio onde algum aspecto do "bem global" é maximizado. Esses modelos podem utilizar uma abordagem probabilística, como a sugerida em [17], onde os jogadores decidem com uma determinada probabilidade qual ação tomar diante das estratégias de seus adversários. Outras abordagens avaliam seus resultados apenas formalmente, como no modelo proposto por Feldman *et al.* em [12], partindo

de uma definição inicial do desempenho do sistema. Em geral, o foco dessas abordagens é coibir os nós oportunistas na rede, mas sem atentar para as propriedades de justiça e confiabilidade do sistema.

Nosso trabalho avança consideravelmente em relação aos trabalhos anteriores, abrangendo situações mais complexas e propondo um mecanismo distribuído e escalável para excluir os nós oportunistas com um enfoque em confiabilidade e justiça na formação das topologias sobrepostas.

CAPÍTULO 3

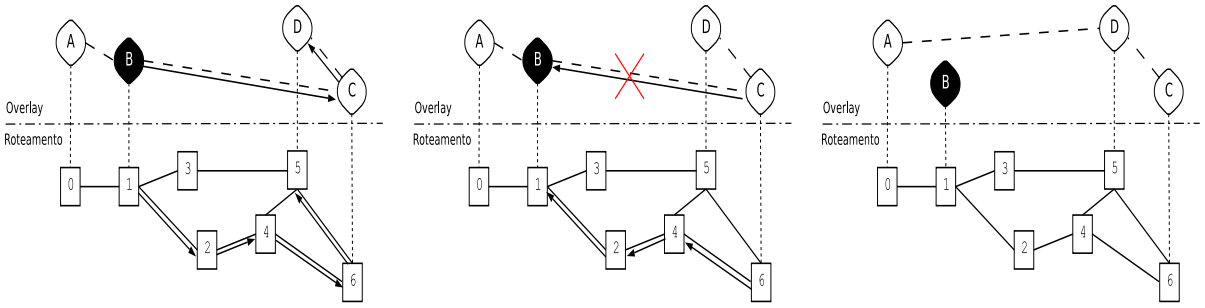
Modelo Proposto

Neste capítulo, detalhamos nossa abordagem para aumentar a confiabilidade em redes sobrepostas com nós egoístas. Primeiramente, fazemos uma breve formulação dos problemas envolvidos e desafios apresentados por eles. Em seguida, descrevemos o conceito de reputação que define a base de nossa abordagem e como os nós podem calculá-lo para definir a confiabilidade de seus pares. Por fim, mostramos como a interação entre os nós é modelada como um jogo não-cooperativo.

3.1 Formulação do Problema

O problema de roteamento sobreposto consiste em encontrar um caminho que satisfaça algumas métricas importantes para a aplicação (máxima largura de banda, mínima latência, máxima confiabilidade, etc) para direcionar o tráfego através dos nós na rede sobreposta. A Figura 3.1 mostra alguns exemplos de redes sobrepostas sobre a mesma topologia física. Na Fig. 3.1, os quadrados denotam os roteadores e nós da rede substrato, enquanto os círculos denotam os nós sobrepostos.

Podemos observar na Fig. 3.1(a) como o nó B usa o roteamento sobreposto para enviar um fluxo de dados para o nó D através do nó C. O problema de roteamento aqui descrito é especialmente efetivo para o roteamento entre Sistemas Autônomos (*Autonomous Systems*). Os *links* entre esses domínios são fundamentais para a operação da rede e são particularmente sensíveis a falhas, ataques e congestionamentos, podendo levar um período potencialmente longo para que as rotas venham a convergir após tais eventos [16]. Redes de roteamento sobrepostas oferecem uma alternativa para o problema da recu-



(a) Nó B é oportunista (em preto) e usa rede sobreposta para rotear tráfego

(b) Nó C tem sua requisição de roteamento negado pelo nó B

(c) Solução possível: nó oportunista excluído

Figura 3.1: Redes Sobrepostas Egoístas

peração rápida do roteamento inter-domínios. Assumimos que os nós na rede sobreposta operam sobre algum protocolo de roteamento específico, que leva em consideração as métricas de interesse da aplicação alvo.

Um princípio básico de uma rede de roteamento sobreposta é que quando os nós disponibilizam seus próprios recursos para algum par na rede, ele pode esperar que os serviços providos serão retribuídos quando requisitados. Na Fig. 3.1(a), por exemplo, o nó B (em preto) usa os recursos de C para rotear seus dados até o nó D. Dessa maneira, C poderia esperar que, já que cedeu seus recursos a B, ele também pode usar os recursos de B para rotear seu próprio tráfego para o nó A. Entretanto, podemos observar na Fig. 3.1(b) uma situação onde essa premissa não se confirma e B decide negar a requisição de C. Este comportamento é possível quando os nós são egoístas e racionais, pois tais nós buscam maximizar seus benefícios e minimizar seus custos. De fato, tornar-se um nó oportunista pode até mesmo ser a melhor estratégia em alguns cenários, se não existem quaisquer incentivos contra isso.

O *problema dos nós oportunistas* consistem em detectar e remover tais nós da rede, pois eles apenas consomem recursos e não contribuem de volta para a comunidade. A Fig. 3.1(c) mostra uma possível solução para tal problema, onde o nó B é excluído e a rede sobreposta é reorganizada para permanecer conexa. Note entretanto, que na prática não é realmente necessário remover todas as conexões com todos os nós oportunistas para retirá-los da rede, já que o mesmo efeito é alcançado se os nós justos pararem de servir as requisições dos *free-riders* e não buscarem usar os seus recursos. Nossa abordagem determina as políticas básicas para a interação entre os nós, que explora sua natureza egoísta para promover a justiça e aumentar a confiabilidade na rede.

3.2 Estratégias Baseadas em Reputação

Quando todos os membros da rede sobreposta agem de forma justa e de acordo com os protocolos pré-definidos, os nós pode confiar completamente uns nos outros. Em tais ambientes, uma requisição não será atendida apenas devido a eventos fora do controle dos nós servidores, tais como falhas, ataques, congestionamentos, etc. A situação se mostra bem diferente em redes sobrepostas egoístas, onde os nós oportunistas não aderem às políticas da rede, colocando em risco a confiabilidade dos serviços oferecidos pelo sistema.

O problema dos nós oportunistas pode ser visto pela perspectiva da confiança. Nesse sentido, nós oportunistas são entendidos como membros da rede que não podem ser confiados pelos outros membros, já que não retribuem os serviços utilizados quando requeridos a fazê-lo. Em nosso modelo, utilizamos o conceito de *reputação* como uma medida de quão justo e confiável um nó é. Um nó racional rapidamente percebe que não há benefícios em ceder recursos a nós não-confiáveis e o mecanismo de reputações é usado justamente para determinar quando um nó deve ou não confiar em um determinado par.

A reputação de um nó determina a probabilidade que este nó possui de ter suas requisições atendidas, e quanto maior a reputação, maior a chance de sucesso. Dessa maneira, os nós possuem um incentivo claro em se mostraem confiáveis e manter a melhor reputação possível. A reputação de cada nó é construída baseada nas *experiências individuais* com o nó e nos *depoimentos dos pares* sobre ele, conceitos que detalharemos a seguir.

3.2.1 Experiência Individual

Definimos a *experiência individual* como a visão pessoal que um nó i possui a respeito da confiabilidade de um outro nó j, baseada apenas nas interações passadas entre eles. Conceitualmente, sempre que i tenta fazer uso dos recursos de um nó j, ele atualiza sua experiência pessoal sobre j, aumentando-a se j age justamente e diminuindo-a em caso contrário. Desta forma, para definirmos formalmente a experiência individual, necessitamos antes delimitar o conceito de *justiça* no contexto da rede sobreposta. Como justiça pode ser um conceito muito subjetivo, nós propomos uma política simples mas bastante efetiva para ser usada na rede.

Definição 1 *Seja $S^t_{i(j)}$ a quantidade de serviços que o nó i forneceu ao nó j até o tempo t. Se i requisita recursos de j, então j é considerado injusto com $i \iff j$ nega a requisição de i e $S^t_{i(j)} - S^t_{j(i)} > 0$.*

A política descrita na Definição 1 torna claro quando um nó no jogo pode considerar outro injusto. Sendo assim, o nó j não é obrigado a atender os

pedidos do nó i se o primeiro tiver provido mais recursos ao último(ex., tráfego roteado) que consumido, isto é, se o *saldo* de recursos providos for positivo para j. Dessa maneira, um jogador pode ser considerado injusto apenas quando não assume os custos associados ao uso de recursos da rede. Evidentemente, a falha de um nó em responder a uma requisição não implica que ele seja necessariamente um nó oportunista. Na realidade, é provável que a maioria dos membros da rede neguem requisições apenas quando realmente não podem honrá-las, devido a causas como falhas de hardware, congestionamentos, falta de recursos, etc. Entretanto, mesmo nesses casos o valor da experiência individual em relação ao nó é decrementado, já que do ponto de vista da aplicação, não importa porque um nó é incapaz de prover um serviço como o esperado. Em outras palavras, a razão pela qual um recurso não pode ser disponibilizado não muda o fato de o nó não se mostrar confiável. De fato, pode ser bastante difícil distinguir quando um nó não *pode* servir uma requisição e quando apenas não o *deseja* fazê-lo. Nós mostramos no Capítulo-4 que ignorar as causas da falha de serviço e se concentrar apenas na questão objetiva de provimento ou não leva a resultados muito bons.

A experiência individual de um nó é formalmente definida na Def. 2.

Definição 2 *Seja $I^t_{i(j)}$ a experiência individual de um nó i em relação a um nó j em um tempo t, $0 \leq I^t_{i(j)} \leq 1$. Seja r a quantidade de recursos requisitada por i, p a quantidade de recursos provida por j e n o número de vezes em que j falhou em processar completamente as requisições de i, $n \geq 1$. Então, $I^t_{i(j)}$ é definida como:*

$$I^t_{i(j)} = \begin{cases} min(I^{t-1}_{i(j)} + \alpha, 1) & \textbf{se } p = r \\ \\ max(I^{t-1}_{i(j)} - (1 - \frac{p}{r})\alpha n^2, 0) & \textbf{se } S_{i(j)} - S_{j(i)} > 0^p! = r \end{cases} \tag{3.1}$$

Como podemos notar na Def. 2, a experiência individual dos jogadores em relação aos outros evolui com o passar do tempo, refletindo o fato de que a estratégia de um jogador (e o seu comportamento) pode variar durante o jogo. Nossa formulação permite tanto variações positivas quanto negativas no valor da experiência individual. O parâmetro α representa o mínimo de *unidades de experiência* envolvidas em cada interação entre os nós i e j, ou seja, o valor mínimo que a experiência individual de i sobre j pode variar em uma interação entre eles.

Existem outros aspectos importantes que podem ser observados na formulação da experiência individual. O primeiro se refere ao quão rapidamente ela cresce e cai. Como pode-se notar na Equação 3.1, enquanto a função cresce linearmente, ela decresce muito mais velozmente. Isso expressa o fato que é muito mais fácil perder credibilidade do que adquirí-la, e incentiva os jogadores a manter bons níveis de reputação e confiabilidade. Isso também

previne os jogadores de se transformarem em nós oportunistas após atingirem altas reputações na rede, já que esse comportamento leva a um rápido decaimento da reputação e a conseqüente perda de acesso aos recursos da rede sobreposta. Ao mesmo tempo, a formulação não impõe altas penalidades a jogadores que falham ocasionalmente em servir alguma requisição. Note que se o nó j não estiver em débito com o nó i, sua experiência individual não é decrescida caso aquele decida negar recursos a este.

Também há de se notar que requisições parcialmente servidas sofrem uma penalidade menor, proporcional a quantidade de recursos negada, como pode ser visto pelo termo $(1 - \frac{p}{r})$. A intenção novamente é não punir excessivamente nós justos, já que uma requisição parcialmente servida é a princípio muito mais provável de se mostrar uma falha do que uma deliberada negação de serviço. Por outro lado, nós que não são oportunistas mas consistentemente falham em responder aos pedidos dos seus pares não podem ser considerados confiáveis, e a formulação leva estes casos em conta, diminuindo a reputação dos nós, conforme seria esperado.

3.2.2 Reputação

Em nosso modelo, a reputação de um nó j é uma métrica de quão confiável um outro nó i o considera, e é usada por i para determinar se é vantajoso prover seus próprios recursos para j em um determinado momento.

Definição 3 *Seja N o número de nós na rede sobreposta e $R^t_{i(j)}, 0 \leq R^t_{i(j)}, \leq 1$ a reputação atribuída por um nó i a um nó j em um tempo t, então $R^t_{i(j)}$ é definida como:*

$$R^t_{i(j)} = R^{t-1}_{i(j)} + \beta_i(T^t_{i(j)} - T^{t-1}_{i(j)}) + (1 - \beta_i)(I^t_{i(j)} - I^{t-1}_{i(j)}) \tag{3.2}$$

onde $T^t_{i(j)}$ é dada por:

$$T^t_{i(j)} = \frac{\sum_{k \in N} I^t_{k(j)} R^t_{i(k)}}{\sum_{k \in N} R^t_{i(k)}} \tag{3.3}$$

Na Def. 3, podemos observar que a reputação de um nó é função de sua reputação anterior e das variações tanto da experiência individual com esse nó quanto na dos *depoimentos dos pares* $T^t_{i(j)}$ a respeito desse nó.

O *depoimentos dos pares*(Eq. 3.3) são simplesmente informações dos outros nós da rede sobre a confiabilidade de um nó em particular, ou em outras palavras, a opinião da comunidade sobre um nó específico. O depoimento de cada nó é ponderado pela sua própria reputação $R^t_{i(k)}$. Assim, a opinião de nós com altas reputações possui maior impacto que aquela de nós com baixas reputações, o que é importante, pois nós com baixas reputações podem ser nós oportunistas que estão tentando maliciosamente difamar nós justos (por não aceitar suas requisições, por exemplo). Como a contribuição de cada nó

para a reputação é proporcional a sua própria reputação, a opinião dos nós oportunistas é diluída e a difamação é evitada.

Assim, um nó pode contar tanto com sua experiência individual na interação com outro par quanto na opinião dos demais membros da rede para inferir a presente confiabilidade daquele par. O parâmetro β_i, $0 \leq \beta_i \leq 1$, é usado para controlar quanta importância um nó i relega à opinião dos seus pares na rede sobreposta e quanta ele atribui a suas próprias experiências anteriores com um nó j. Portanto, valores altos de β_i enfatizam os depoimentos dos pares na definição da reputação, enquanto valores baixos de β_i dão mais peso à experiência individual. É fácil perceber pela Eq. 3.2 que a reputação de um nó não é unicamente definida em toda rede sobreposta, mas ao invés disso, construída individualmente por cada nó, baseada em diferentes fontes de dados. Nós mostramos que, embora não haja o conceito de reputação global na rede, nosso mecanismo leva a vasta maioria dos nós a atribuir baixas reputações aos nós oportunistas e excluí-los da rede sobreposta, aumentando assim a confiabilidade dos serviços providos.

3.3 Uma Abordagem Baseada em Teoria dos Jogos

Nós modelamos a interação entre os n nós da rede sobreposta como um jogo não-cooperativo, onde cada nó é um jogador cuja estratégia se baseia em selecionar os vizinhos para se conectar de forma a maximizar seus benefícios. Cada jogador inicia o jogo com a reputação de 0,5, que representa uma taxa de confiança padrão, ou seja, o nó nem é considerado extremamente confiável ou trapaceiro a princípio. Cada jogador também possui um *nível mínimo de reputação*, como mostrado na Def. 4.

Definição 4 *Seja P o conjunto de jogadores, então $\forall i \in P, \exists$* nível mínimo de reputação $R_{min(i)}$, $0 \leq R_{min(i)} < 0,5$, *tal que se $R^t_{i(j)} < R_{min(i)}$, então i não interage com j.*

Se a reputação de um jogador cai abaixo do nível mínimo de reputação exigido pelo outro nó com o qual ele deseja interagir, então todas as requisições do jogador são negadas por esse nó. Mais ainda, um nó nem ao menos forma conexões com jogadores cuja reputação não obedecem ao critério de reputação mínima e também nunca tenta usar os recursos destes jogadores, já que eles são identificados como oportunistas. Observe que como cada jogador começa o jogo com a reputação de 0,5 e $R_{min(i)} < 0,5$ por definição, todos os jogadores são considerados confiáveis no começo do jogo.

A reputação mínima $R_{min(i)}$ pode ser vista como uma medida individual de risco que o jogador i está disposto a assumir quando compartilha seus recursos. Assim, enquanto alguns jogadores podem ser conservadores em relação

à confiabilidade dos seus pares, outros podem aceitar prover serviços a nós de reputação duvidosa em prol de possíveis maiores benefícios, como menores taxas de latência, por exemplo. Na verdade, tanto valores muito altos de R_{min} quanto valores muito baixos provavelmente levam a estratégias ruins: o primeiro porque restringe significamente o número de jogadores aceitáveis, podendo inclusive levar a uma "exclusão voluntária" da rede; o último porque é muito suscetível a nós oportunistas. Entretanto, é fundamental para a operação do modelo que existam esses diferentes níveis mínimos de reputação para cada nó, já que os jogadores mais rígidos são os primeiros a negar recursos a nós oportunistas, enquanto jogadores que exigem baixos níveis de reputação tornam possível incluir de volta nós que adquiriram uma má reputação no passado, aceitando suas requisições e divulgando seu novo comportamento caso este tenha se alterado. Assim, um nó oportunista pode se reabilitar na rede se modificar seu próprio comportamento, e o compartilhamento de recursos com os demais nós torna-se possível tão logo sua reputação ultrapasse o nível mínimo de cada outro jogador. Isso é garantido pela função de utilidade, como veremos a seguir.

3.3.1 Função de Utilidade

A função de utilidade é um dos mais importantes componentes do jogo e matematicamente caracteriza os interesses dos jogadores quantificando os benefícios trazidos por cada estratégia analisada. Uma função de utilidade poderia considerar, por exemplo, a latência da conexão entre dois nós sobrepostos para avaliar o quão boa ela é. Comparativamente, poderíamos usar a *latência relativa*(Def. 5) da conexão, isto é, a latência da conexão com um nó j comparada com a latência da melhor conexão possível que o jogador i poderia estabelecer na rede sobreposta. Dessa maneira, a função de utilidade poderia ser definida como o inverso da latência relativa (i.e., $1/L^t_{i(j)}$), de forma que quanto menor a latência relativa, maior o valor da função de utilidade e os benefícios associados àquela conexão. Essa formulação satisfaz o caráter racional e egoísta dos nós, já que vai de encontro ao desejo destes de maximizar seus benefícios com as melhores conexões possíveis.

Definição 5 *No tempo t, seja $l^t_{i(j)}$ a latência de uma conexão entre o nó i e o nó j, e seja $l^t_{min(i)}$ a latência mínima de qualquer conexão que i pode estabelecer em t com qualquer outro nó sobreposto. Então, a* latência relativa $L^t_{i(j)}$ *de uma conexão entre i e j é dada por:*

$$L_{i(j)^t} = \frac{l^t_{i(j)}}{l^t_{min(i)}} \tag{3.4}$$

Entretanto, em muitos casos o desempenho teoricamente ótimo da rede requer conexões com nós oportunistas, assumindo que essas conexões são tão boas ou melhores que aquelas com nós justos. Como esse nós nunca provêm seus próprios recursos para a rede, essas conexões se mostram inúteis e o desempenho real da rede é muito pior que o dado pelo limite ótimo. De fato, os nós oportunistas não apenas afetam o desempenho da rede, como diminuem significativamente a confiabilidade dos serviços, já que a princípio um nó não pode dizer se há ou não um nó oportunista no caminho escolhido por ele para rotear seus pacotes. A segunda parte da função de utilidade leva em conta essas situações, incorporando o conceito de reputação no jogo. Assim, nossa função de utilidade se torna:

$$u^t_{i(j)} = \begin{cases} \frac{R^t_{i(j)}}{L_{i(j)^t}} & \text{if } R^t_{i(j)} > R_{min(i)} \\ \\ -\infty & \text{caso contrário} \end{cases} \tag{3.5}$$

Torna-se claro quando observamos a Eq. 3.5 porque o nó i não interage com jogadores cuja reputação é menor que $R_{min(i)}$: o benefício esperado é $-\infty$. O objetivo primordial dos jogadores passa a ser estabelecer conexões de baixa latência com nós *confiáveis*. Possivelmente, boas conexões apresentam um compromisso entre esses dois requisitos, já que tanto *links* para nós de alta reputação e alta latência quanto conexões com nós de baixa reputação e baixa latência são provavelmente desinteressantes, embora por diferentes razões.

A função de utilidade é usada por cada jogador i para determinar sua estratégia, que é o conjunto de nós escolhidos para se conectar. O benefício total do grafo G formado usando a estratégia s em um tempo t é dado por:

$$B^t_i(G) = \sum_{j \in C_s} u^t_{i,j} \tag{3.6}$$

onde C_s é o conjunto de nós selecionados pela estratégia s. Essa é a função que os jogadores tentam maximizar.

3.3.2 Modelo do Jogo

Em nosso modelo, nós descartamos o uso de uma abordagem estrita de teoria dos jogos, que assume um ambiente onde todas as informações são conhecidas (como em um jogo de xadrez) em favor de um jogo com informações incompletas, onde cada jogador não está ciente das estratégias e objetivos uns dos outros. Nós acreditamos que essa abordagem melhor descreve um ambiente competitivo em redes sobrepostas egoístas.

Assumimos que os jogadores executam suas estratégias sem erros, que o jogo corretamente descreve os benefícios buscados pelos jogadores e que cada

jogador acredita que todos os outros jogadores também são racionais e egoístas. Nash demonstrou que todo jogo com tais características possui um equilíbrio de Nash, que é o conjunto de *estratégias puras* (neste jogo, conexões) escolhidas por cada jogador [21]. Dessa maneira, as topologias finais da rede sobreposta se encontram são o resultado do equilíbrio de Nash do jogo e nós mostramos que nós oportunistas estão virtualmente ausentes nessas topologias.

Nosso mecanismo demanda que cada jogador tenha ao menos duas conexões, com nós distintos na rede sobreposta. Com ao menos duas conexões, todos os nós têm condições de rotear tráfego e torna-se mais difícil para os nós oportunistas evitarem suas responsabilidades na rede simplesmente se tornando folhas no grafo da topologia da rede. Assim, considera-se que nós que divulgam menos de duas conexões trazem um benefício de $-\infty$ e o acesso aos recursos da rede é conseqüentemente negado a tais nós. O uso dessa política é outra maneira de reforçar a justiça no sistema.

Início do Jogo

O jogo acontece através de um procedimento iterativo, onde em cada rodada os jogadores tomam suas decisões baseados na percepção atual da rede. Dessa forma, eles selecionam quais ações tomar em seguida, com adicionar ou remover conexões com outros nós e atribuir reputações a seus pares. O jogo inicia-se como um grafo aleatoriamente conexo e em cada rodada, cada jogador modifica sua estratégia (o conjunto de conexões estabelecidas) para maximizar seus benefícios. O equilíbrio de Nash é alcançado quando todos os jogadores mantém suas estratégias inalteradas em uma rodada e a topologia final da rede sobreposta é obtida.

As ações tomadas por cada jogador no início de cada rodada são descritas no Algoritmo 1.

Algorithm 1 Ações iniciais do jogador i em cada rodada

```
1: C ← nós cujas reputações se alteraram t − 1
2: for all nó j ∈ C do
3:    Atualiza reputação R^t_{i(j)}
4: end for
5: for all nó j conectados a i do
6:    Compute u^t_{i(j)}
7:    if u^t_{i(j)} = −∞ then
8:       Remove a conexão entre i e j
9:    end if
10: end for
```

Primeiramente, o jogador atualiza a reputação de todos os outros jogadores cujas reputações foram alteradas na rodada anterior. Essa informação é re-

cebida após as interações entre os nós, anexadas nos pacotes regulares do protocolo de roteamento da rede sobreposta. Dessa maneira, os jogadores possuem informações atuais sobre o comportamento dos nós na rede.

Com as reputações atualizadas, os jogadores recalculam os benefícios trazidos por cada conexão mantida por ele. Os benefícios trazidos pelas conexões podem ter sido alterados tanto devido à mudanças na latência dos *links* (como por congestionamentos, por exemplo) quanto na alteração da reputação dos pares. Se a reputação do nó com o qual a conexão é mantida cai abaixo do nível mínimo de reputação exigido pelo nó, a conexão é removida.

Escolha de Estratégias

Após executar as ações no Algoritmo 1, o jogador começa efetivamente a buscar no universo de estratégias possíveis melhores configurações, como a adição de melhores conexões a remoção das piores. O procedimento é mostrado no Alg. 2.

Algorithm 2 Escolha da estratégia do jogador i

1: **for all** nó $j \in$ rede sobreposta **do**
2: **if** $R^t_{i(j)} > R^t_{min(i)} \wedge R^t_{j(i)} > R^t_{min(j)}$ **then**
3: Computa $B^t_i(G)$ com uma nova conexão com j
4: **if** $B^t_i(G) - B^{t-1}_i(G) > \gamma$ **then**
5: Adiciona j
6: $B^{t-1}_i(G) \leftarrow B^t_i(G)$
7: **end if**
8: **end if**
9: **end for**
10: **for all** conexão c que i possui **do**
11: **if** número de conexões > 2 **then**
12: Computa $B^t_i(G)$ desconsiderando c
13: **if** $B^{t-1}_i(G) - B^t_i(G) < \gamma$ **then**
14: Remove c
15: $B^{t-1}_i(G) \leftarrow B^t_i(G)$
16: **end if**
17: **end if**
18: **end for**

Para escolher a melhor estratégia no tempo t, cada nó avalia quais novas conexões podem ser vantajosas e quais conexões atualmente estabelecidas trazem poucos benefícios e podem ser seguramente removidas. O procedimento mostrado no Alg. 2 pode ser dividido em duas partes.

Na primeira (linhas 1-9), o jogador i calcula o benefício de cada possível conexão ainda não estabelecida com os outros nós sobrepostos. Primeiramente, i checa se a reputação do jogador j, com quem ele quer estabelecer uma conexão, encontra-se acima do nível mínimo de reputação exigido. Como

anteriormente detalhado, i conta com informações recentes da rede para determinar a confiabilidade de j e não estabelece a conexão se o critério de reputação mínimo não for respeitado. Entretanto, não é suficiente que i aceite j como um nó confiável, é necessário que j também acredite que i não é um nó oportunista que vai apenas se aproveitar de seus recursos. Se ambas as condições são verdadeiras, a criação da conexão se torna possível e i calcula os ganhos total do grafo com o novo *link* adicionado (Eq. 3.6). A conexão é definitivamente adicionada se o ganho trazido é maior que um limite definido γ.

Na segunda parte do Alg. 2 (linhas 9-18), o jogador avalia quais conexões anteriormente estabelecidas podem ser removidas, desde que pelo menos duas outras conexões continuem operacionais. Uma conexão pode ser removida se sua retirada implica em perdas menores que um determinado limite, ou em outras palavras, se os benefícios trazidos por aquela conexão são menores que γ, um limiar dependente do tamanho da rede sobreposta. Outros protocolos que levam à criação de topologias de redes sobrepostas também usam uma avaliação periódica das conexões e um limite dependente do número de nós para adicionar ou remover conexões [5, 4].

Quando a estratégia é finalmente consolidada, o jogador pode começar a usar os serviços da rede sobreposta e ajustar a experiência pessoal dos outros nós com o qual interage de acordo com o comportamento desses nós, conforme o mecanismo descrito na Def. 2. Após utilizar os serviços desejados, o jogador faz um *broadcast* da reputação recalculada dos nós envolvidos nas recentes interações para o restante dos pares na rede. Essa informação é transmitida via o mecanismo usual de roteamento sobreposto, que já faz uso de *broadcasts* periódicos para divulgar as informações sobre *links* e rotas. Dessa forma, muita pouca carga adicional é introduzida no sistema.

CAPÍTULO 4

Avaliação Experimental

Para avaliar o mecanismo proposto, fizemos simulações extensivas do modelo para analisar as propriedades de confiabilidade e justiça das topologias resultantes do equilíbrio de Nash. Os resultados foram gerados através da média de pelo menos 300 simulações distintas usando o mesmo conjunto de parâmetros iniciais. A topologia da rede IP que constitui a camada substrato da rede sobreposta foi obtida mapeando a conectividade da rede PlanetLab de vários pontos diferentes, obtendo 3477 nós e 5049 conexões. O PlanetLab é uma infraestrutura mundial para testes e experimentos com serviços de rede, e as métricas de latência e consumo de banda também foram geradas a partir dessa rede. Por simplicidade, nossas simulações consideram um "instantâneo" da rede, de forma que as latências são tidas como constantes para que possamos isolar e analisar as variações nos parâmetros do nosso modelo.

Para iniciar a simulação, inicialmente escolhemos aleatoriamente 100 nós da topologia substrato para formar a rede sobreposta e associamos aqueles com a menor latência aos nós oportunistas. Dessa maneira, os nós oportunistas se tornaram pontos preferenciais de conexão, o que nos possibilitou analisar os possivelmente piores cenários, onde estes nós são altamente conexos e freqüentemente escolhidos pelos demais nós da rede para rotear dados. Nós justos também possuem uma probabilidade de 3% de não conseguir responder às requisições, simulando assim períodos de negação involuntária de recursos (como falhas de hardware, congestionamentos, etc.), quando os nós justos aparentemente se comportam como oportunistas. Esperamos que nosso mecanismo consiga distinguir esses casos de nós realmente oportunistas.

O valor do nível mínimo de reputação é uniformemente distribuído entre

os jogadores. Após cada jogador reestruturar suas conexões de forma a maximizar os benefícios trazidos pelo grafo da topologia, ele passa então a utilizar a rede, probabilisticamente enviando tráfego para até 10% dos demais nós da rede sobreposta, aleatoriamente escolhidos.

4.1 Métricas

As seguintes métricas foram avaliadas.

- *Serviço Provido a Nós Oportunistas*: Essa métrica mostra a evolução dos jogadores que se dispõe a prover serviços da rede sobreposta aos nós oportunistas, conforme o jogo progride. Idealmente, nenhum serviço deve ser provido ou requisitado aos nós oportunista, o que na prática os excluiria da rede e aumentaria a confiabilidade e qualidade dos serviços para os nós justos. Essa métrica mostra a eficiência de uma estratégia em detectar e remover nós oportunistas.

- *Serviço Provido aos Nós Justos*: Similar a métrica acima, ela mostra a porcentagem média de nós justos dispostos a prover serviço aos demais nós justos da rede. Essa métrica mostra o quão suscetível uma estratégia é a falso-positivos, isto é, a nós justos incorretamente assinalados como oportunistas.

- *Nós Alcançáveis*: Definidos como a porcentagem média de nós justos que cada um dos outros nós justos consegue alcançar. Claramente, se um nó justo depende de um oportunista para rotear seu tráfego para qualquer outro par, este par é provavelmente inalcançável, visto que nós oportunistas não respondem as requisições de roteamento.

- *Confiabilidade*: Definida como a razão entre a quantidade de recursos requisitados e a quantidade de recursos recebidos, esta métrica provém informações sobre a qualidade e confiabilidade dos serviços providos pela rede sobreposta. Valores próximos a um significam um sistemas com topologias altamente confiáveis, enquanto valores próximos a zero indicam uma alta incidência de nós oportunistas.

- *Número de Partições*: Definido como o número médio de partições na topologia final da rede sobreposta devido a presença de nós oportunistas. Uma partição é formada se ao menos um nó justo depende de um oportunista para alcançar qualquer outro na rede, já que nós oportunistas não provém serviços. Os nós sobrepostos podem alcançar membros da rede apenas na mesma partição em que eles se encontram, e a medida

Estratégia	Função de Utilidade
Gulosa	$\frac{1}{L^t_{i(j)}}$ (eq. 3.4)
Probabilística	$\frac{1}{L^t_{i(j)}} \iff P(j) > \frac{1}{2^n}$
Reputação	$u_{i(j)}$ (eq. 3.5)

Tabela 4.1: Estratégias avaliadas com suas respectivas funções de utilidade

que o número de partições cresce a quantidade de nós alcançáveis drasticamente diminui, em conjunto com a confiabilidade da rede em rotear tráfego para qualquer um dos seus membros.

4.2 Estratégias Avaliadas

Para avaliar a eficácia da nossa abordagem, comparamos nosso mecanismo com duas outras estratégias. Nas simulações, variamos o parâmetro β para estudar seu impacto no comportamento do sistema. O parâmetro α foi analisado a parte. Descrevemos todas as estratégias avaliadas abaixo, e sumarizamos a função de utilidade de cada um delas na Tabela 4.1.

- *Gulosa*: Essa provavelmente seria uma das estratégias mais usadas em uma rede sobreposta egoísta convencional. A função de utilidade é dada apenas em termos da latência relativa e os jogadores não tentam identificar nós oportunistas, assumindo que todos os membros da rede são igualmente confiáveis.

- *Probabilística*: Nesta estratégia, os jogadores não apenas consideram a latência relativa, como também probabilisticamente decidem estabelecer conexões ou não com outros jogadores e prover recursos a eles baseado em interações passadas. Um jogador A tem uma chance de $1/2^n$ de cooperar com um outro jogador B, onde $n \geq 0$ representa o número de vezes em que as requisições de A foram negadas por B.

- *Reputação*: Estratégia proposta nesse estudo, que define a confiabilidade dos nós e os benefícios trazidos por cada conexão de acordo com o modelo descrito no Cap. 3

4.3 Avaliação Experimental

Primeiramente, verificamos o impacto do parâmetro α do nosso modelo para os serviços providos aos nós oportunistas. A Fig. 4.1 mostra as curvas resultantes da variação deste parâmetro. Podemos observar que a medida em

que o valor de α aumenta, a reputação dos jogadores sobe e cai mais rapidamente. Este fato se relaciona ao tempo médio de convergência do jogo. Já que em média nossas simulações levaram aproximadamente o mesmo número de rodadas para alcançar o equilíbrio de Nash, valores mais altos de α impuseram penalidades mais pesadas sobre nós oportunistas no mesmo período de tempo. Assim, os nós oportunistas terminaram o jogo com reputações menores, o que por sua vez fez com que mais jogadores se negassem a prover serviços para estes nós. Nos experimentos seguintes, mantivemos $\alpha = 0.05$.

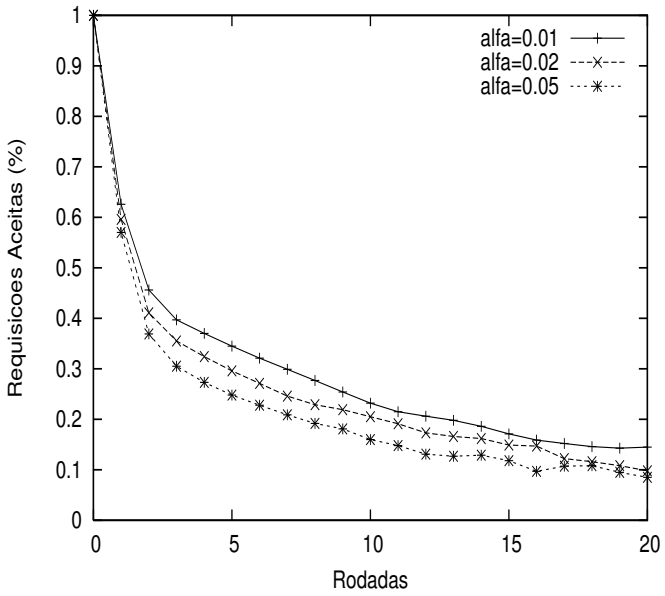


Figura 4.1: Requisições aceitas variando-se α

A Fig. 4.2 nos mostra o serviço provido aos nós oportunistas ao longo das simulações com o uso de diferentes estratégias. A estratégia *gulosa* leva todos os jogadores a sempre servir as requisições dos nós oportunistas, o que é esperado, já que nenhuma tentativa de identificação de nós oportunistas é realizada nesta estratégia. A abordagem *probabilística* mostra-se mais efetiva que a *gulosa*, e o sistema é capaz de negar o acesso a recursos a uma parte significativa dos nós oportunistas. Entretanto, é a função de utilidade baseada em reputação que mais eficientemente previne que os nós oportunistas tenham acesso aos serviços da rede sobrepostas, com menos de 5% dos nós justos ainda aceitando responder às requisições dos nós oportunistas quando $\beta = 1$. Note também que quanto maior o valor de β, ou seja, quanto mais informação providas pela rede os nós usam, mais efetiva é a estratégia em isolar os nós oportunistas. Essa é uma tendência que se repete nos outros experimentos realizados, como veremos a seguir.

Um mecanismo de detecção de nós oportunistas não deve apenas identificar jogadores injustos, mas também corretamente distinguí-los de jogadores justos, e assegurar que estes não sejam incorretamente penalizados. A Fig. 4.3

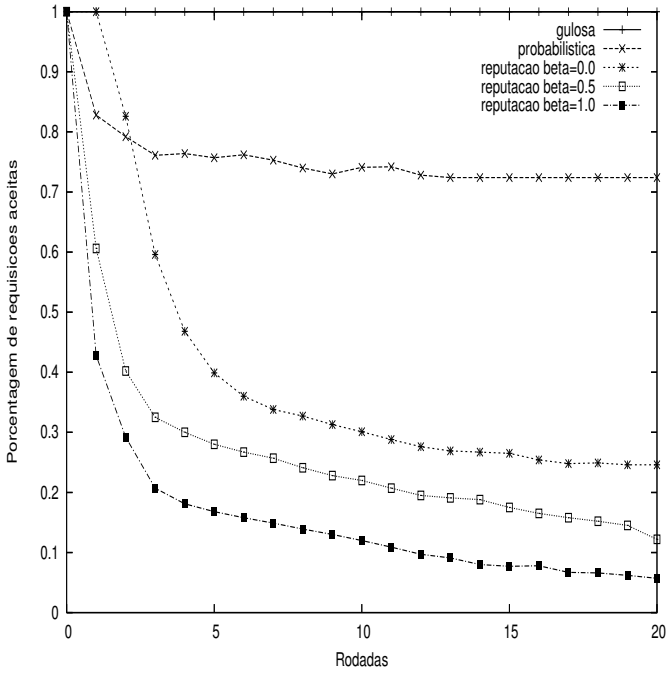


Figura 4.2: Serviço provido aos nós oportunistas

mostra que todas as estratégias promovem um bom comportamento em relação a disposição dos jogadores em prover serviços a nós justos. Basicamente, esses nós não são confundidos com nós oportunistas por seus pares, e quase sempre tem as suas requisições respondidas pelos outros jogadores justos.

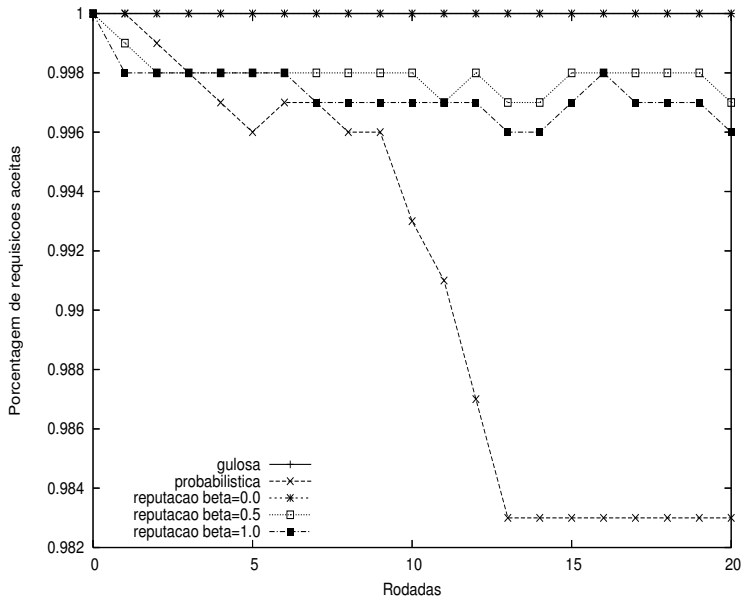


Figura 4.3: Serviço provido aos nós justos

Entretanto, não basta que que as requisições de roteamento sejam aceitas pelos nós justos, é necessário que o caminho escolhido não contenha nenhum nó oportunista, já que eles não provém serviços e tornam inalcançáveis qual-

quer nó após aquele ponto da rota. Podemos observar a porcentagem média de nós alcançáveis por cada jogador na Fig. 4.4. Note que no primeiro ponto, o grafo foi conectado aleatoriamente e os nós são alcançáveis, e só da segunda rodada em diante é que os *links* e conexões são escolhidos pelos próprios nós. A estratégia baseada em *reputação* claramente supera as demais avaliadas, assegurando que não sejam estabelecidas conexões com nós oportunistas e conseqüentemente formando rotas compostas apenas de nós justos. É interessante notar que embora os serviços possivelmente disponíveis para os nós justos seja muito substancial tanto na estratégia *probabilística* quanto na *gulosa*(Fig.4.3), ambas falham em impedir que os jogadores estabeleçam conexões com nós oportunistas, e portanto o número de nós alcançáveis é bem menor que o esperado.

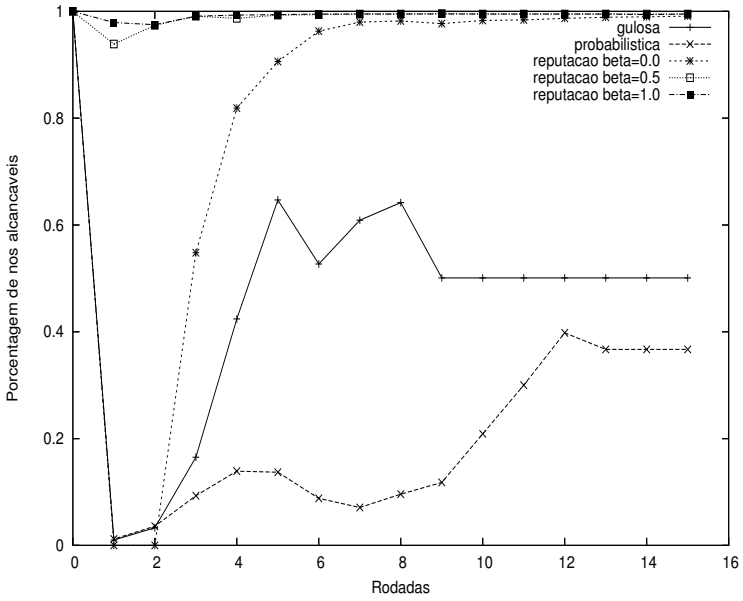


Figura 4.4: Nós Alcançáveis

Essa situação é melhor entendida quando observamos a amostra de uma das topologias geradas nas nossas simulações (Fig. 4.3). Os nós oportunistas foram destacados em preto. Quando não há restrições no grau de conexões dos nós e os jogadores buscam apenas estabelecer conexões que tragam grandes benefícios, a maioria dos nós prefere se conectar a apenas um nó, possivelmente aquele com a menor latência, formando topologias em estrela. Se um nó oportunista torna-se o centro da estrela, todas as rotas devem incluí-lo como um *hop*. Como estes nós recusam todas as requisições de roteamento, a maioria dos nós sobrepostos tornam-se inalcançáveis na prática. Isso não acontece nas estratégias baseadas em *reputação*, como visto na topologia exemplo na Fig. **??**. Embora as topologias ainda se assemelhem a estrelas, são formados múltiplos centros altamente conexos, garantindo assim um aumento significativo no número de rotas disponíveis. Mais ainda, devido ao fato dos nós

oportunistas adquirirem reputações muito baixas durante o jogo, o benefício de se estabelecer conexões com eles é baixo, e portanto eles nunca se tornam pontos preferenciais de ligação no sistema. Assim, os nós oportunistas têm chances muito pequenas de ser um dos centros da topologia

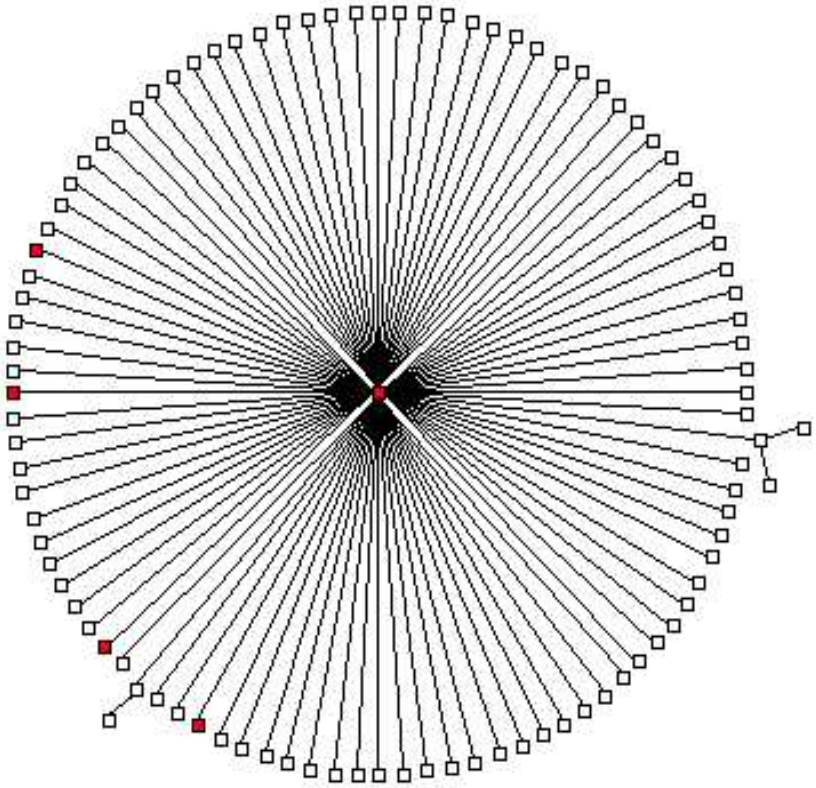


Figura 4.5: Amostra de topologia gerada pela estratégia gulosa (nós oportunistas em preto)

A *confiabilidade* dos serviços providos em função das topologias resultantes é mostrada na figura Fig. 4.7. Em uma rede sobreposta completamente confiável, todos os serviços são providos e a razão da confiabilidade equivale a 1. Entretanto, a presença e atuação dos nós oportunistas impacta severamente a capacidade da rede de responder à demanda dos seus membros. Tanto as estratégia *probabilística* quanto a *gulosa* apresentam índices muito baixo de confiabilidade. O problema piora quando a porcentagem de nós oportunistas na rede aumenta, e com 10% deles, praticamente nenhuma requisição consegue ser executada com sucesso. Por outro lado, nosso mecanismo é capaz de gerar topologias livre de nós oportunistas, que pode aumentar a confiabilidade das requisições submetidas para até 95%, mesmo diante de altas porcentagens de nós oportunistas na rede.

Finalmente, a Fig. 4.8 mostra o número de partições criada no grafo da rede pelo uso de cada estratégia. Novamente, o mecanismo baseado em *reputação*

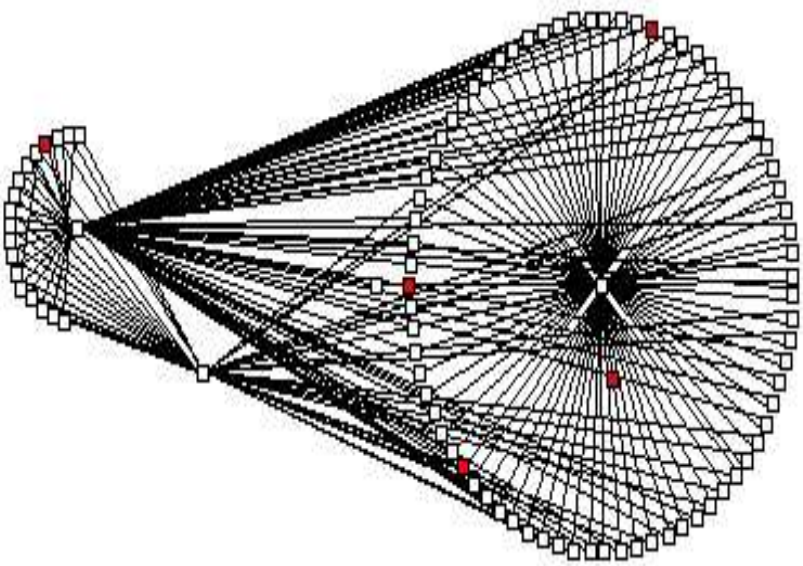


Figura 4.6: Amostra de topologia gerada pela estratégia baseada em reputação (nós oportunistas em preto)

supera as outras estratégias, podendo criar topologias não particionadas na maioria dos casos. Partições na rede limitam drasticamente o número de nós alcançáveis, e se os nós justos não tem consciência da presença dos oportunistas e do particionamento criado por eles, o problema torna-se ainda mais grave, pois requisições que não serão respondidas continuarão a ser feitas para os nós oportunistas. Nossa abordagem impede que isso aconteça através da exclusão desses nós das rotas na rede sobreposta.

Um fato constantemente observado nos experimentos é que quanto mais informações providas pelos outros jogadores um nó usa para determinar as reputações de seus pares, maior a eficácia da estratégia e a conseqüente exclusão dos nós oportunistas e aumento da confiabilidade dos serviços da rede. A razão para esta melhora é clara: considerar os dados providos pelos pares leva a uma atualização muito mais rápida e acurada da visão do jogador sobre a rede do que levar em conta apenas as interações do próprio jogador (valores de β próximos a zero).

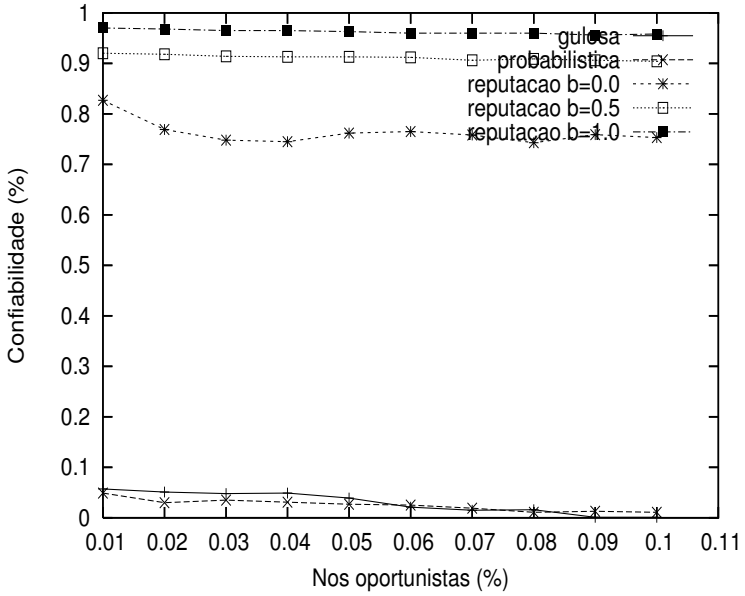


Figura 4.7: Índice de Confiabilidade

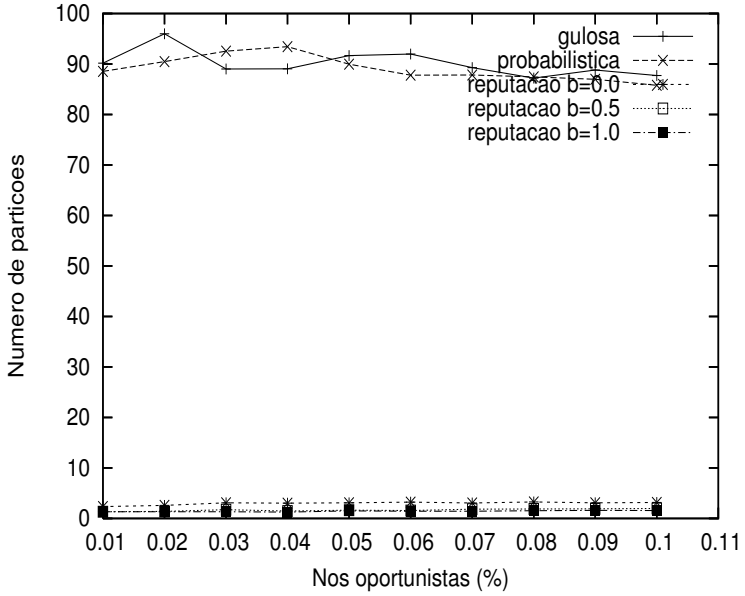


Figura 4.8: Número médio de partições na rede sobreposta

CAPÍTULO 5

Conclusão e Trabalhos Futuros

Apresentamos aqui as conclusões gerais do nosso estudo e algumas possíveis direções para trabalhos futuros.

5.1 Conclusões

Nesta dissertação, apresentamos uma nova abordagem baseada no conceito de reputação para aumentar a confiabilidade e justiça em redes sobrepostas com nós egoístas. Através de uma modelagem baseada em jogos não-cooperativos, avaliamos a eficácia da nossa abordagem e a testamos em comparação com outras estratégias e funções de utilidade.

Verificamos que o nosso mecanismo é efetivamente capaz de impedir que os nós oportunistas drenem os recursos da rede sobreposta, sem que com isso os nós justos sejam incorretamente penalizados. Verificamos que o nosso mecanismo pode levar a um aumento de confiabilidade de serviços para até 95%, mesmo com uma alta porcentagem de nós oportunistas na rede, e que o uso de informações providas pelos pares aumenta significativamente a eficiência do mecanismo em oposição ao uso limitado de informações e experiências individuais para a determinação da reputação dos pares.

5.2 Trabalhos Futuros

Existem várias direções promissoras para trabalhos futuros. O mecanismo de reputações é sujeito a diversos ataques quando as não são constantes e perenes, o que é especialmente quando a rede é dinâmica e os nós podem se juntar ao sistema e deixá-lo livremente. Pretendemos estudar mecanismos

que impeçam que um jogador possa se livrar da má reputação adquirida ao deixar a rede e juntar-se a ela novamente com uma nova identidade (estratégia conhecida como *whitewashing*). Trabalhos anteriores [14] indicam que impor sanções em recém-chegados pode prevenir esse tipo de comportamento (embora às custas de uma penalidade social), e pretendemos analisar como tal mecanismo pode ser incorporado ao nosso modelo.

Outro ataque relacionado à persistência de identidades é aquele onde um único nó obtém várias identidades distintas na rede e se apresenta como múltiplas entidades diferentes, influindo assim consideravelmente no funcionamento dos protocolos e políticas definidos pelo sistema (*sybil attack*). Embora alguns trabalhos argumentem que a única forma de se prevenir esse tipo de ataque é via certificação em uma entidade logicamente centralizada [9], ainda é uma questão em aberto se a imposição de penalidades a recém-chegados pode tornar este ataque tão caro a ponto de torná-lo impraticável.

Também intencionamos avaliar nossa abordagem em ambientes dinâmicos de latência, incorporando congestionamentos e flutuações no tráfego e número de membros nas nossas simulações, já que em nossos experimentos consideramos apenas um cenário estático para melhor isolar os parâmetros e funções de custo envolvidas no modelo.

Outra análise interessante é verificar como a atuação conjunta dos nós oportunistas pode afetar o mecanismo de reputações. Assumimos aqui que não há coordenação entre os nós oportunistas e que eles tentam individualmente tirar proveito da rede sobreposta, o que acreditamos ser o caso mais comum. Entretanto, nada impede que esses nós se agrupem e tentem ludibriar as políticas da rede em conjunto, divulgando avaliações onde eles mutuamente se afirmam como nós confiáveis, por exemplo. Estudar a prevenção desse tipo de ataque é uma interessante linha de pesquisa.

De fato, não é realmente viável dizer que uma política ou estratégia pode efetiva e definitivamente eliminar a presença de nós oportunistas da rede, já que existe uma miríade de ataques possíveis, muitos deles ainda nem ao menos conhecidos. Em um aspecto muito semelhante ao que ocorre na esfera de segurança de sistemas, o principal objetivo dos mecanismos e estratégias propostas é aumentar as dificuldades impostas para que ataques e usos indevidos não aconteçam, de maneira a forçar os ofensores a buscar estratégias cada mais complexas e caras para conseguir seus objetivos. O estudo dos possíveis ataques e implicações de cada política e protocolo oferece inúmeras possibilidades de pesquisa.

Referências Bibliográficas

[1] D. G. ANDERSEN, H. BALAKRISHNAN, M. F. KAASHOEK, AND R. MORRIS, *Resilient overlay networks*, in Symposium on Operating Systems Principles, 2001, pp. 131–145.

[2] R. AXELROD, *The Evolution of Cooperation*, Basic Books, New York, 1984.

[3] S. BUCHEGGER AND J.-Y. L. 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, IEEE.

[4] Y. CHAWATHE, *Scattercast: An architecture for internet broadcast distribution as an infrastructure service*, 2000.

[5] Y.-H. CHU, S. G. RAO, AND H. ZHANG, *A case for end system multicast*, in Measurement and Modeling of Computer Systems, 2000, pp. 1–12.

[6] B. CHUN, R. FONSECA, I. STOICA, AND J. KUBIATOWICZ, *Characterizing selfishly constructed overlay networks*, in Proceedings of IEEE INFOCOM'04, Hong Kong, 2004.

[7] B. COHEN, *Incentives build robustness in bittorrent*, 2003.

[8] P. DARAS, D. PALAKA, V. GIAGOURTA, D. BECHTSIS, K. PETRIDIS, AND M. G. STRINTZIS, *A novel peer-to-peer payment protocol*, in Proceedings of IEEE EUROCON, 2003.

[9] J. DOUCEUR, *The sybil attack*, in In Proceedings of the IPTPS02 Workshop, Cambridge, USA, March 2002.

[10] A. FABRIKANT, A. LUTHRA, E. MANEVA, C. PAPADIMITRIOU, AND S. SHENKER, *On a netowrk creation game*, in Proceedings of ACM PODC, ACM Press, New York, 2003.

[11] J. FEIGENBAUM AND S. SHENKER, *Distributed algorithmic mechanism design: Recent results and future directions*, in Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, ACM Press, New York, 2002, pp. 1–13.

[12] M. FELDMAN, C. PAPADIMITRIOU, J. CHUANG, AND I. STOICA, *Free-riding and whitewashing in peer-to-peer systems*, in Proceedings of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems, Portland, Oregon, USA, 2004, ACM Press.

[13] E. FRIEDMAN, *Selfish routing on data networks isn't too bad: genericity,tcp and ospf*, tech. rep., 2002.

[14] E. FRIEDMAN AND P. RESNICK, *The social cost of cheap pseudonyms*, Journal of Economics and Management Strategy, 10 (1998), pp. 173–199.

[15] P. GOLLE, K. LEYTON-BROWN, I. MIRONOV, AND M. LILLIBRIDGE, *Incentives for sharing in peer-to-peer networks*, Lecture Notes in Computer Science, 2232 (2001), pp. 75+.

[16] C. LABOVITZ, A. AHUJA, A. BOSE, AND F. JAHANIAN, *Delayed internet routing convergence*, in SIGCOMM, 2000, pp. 175–187.

[17] K. LAI, M. FELDMAN, I. STOICA, AND J. CHUANG, *Incentives for cooperation in peer-to-peer networks*, in In Workshop on Economics of Peer-to-Peer Systems, 2003.

[18] Z. LI AND P. MOHAPATRA, *Hostcast: A new overlay multicasting protocol*, in In Proc. IEEE Int. Communications Conference (ICC'03), 2003.

[19] ——, *Qron: Qos-aware routing in overlay networks*, IEEE JSAC, (2003).

[20] S. N. LTD.., *Kazaa network*, 2003.

[21] J. F. NASH, *Non-cooperative games*, in Annals of Mathematics, March 1951, pp. 286–295.

[22] C. PAPADIMITRIOU, *Algorithms, games and the internet*, in 33rd Anual ACM Symposium on the Theory of Computing, 2001, pp. 749–753.

[23] M. RIPEANU, *Peer-to-peer architecture case study: Gnutella network*, 2001.

[24] T. ROUGHGARDEN AND E. TARDOS, *How bad is selfish routing?*, Journal of the ACM, (2002), pp. 236–259.

[25] A. ROWSTRON AND P. DRUSCHEL, *Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems*, in IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), 2001, pp. 329–350.

[26] S. SAVAGE, T. ANDERSON, A. AGGARWAL, D. BECKER, N. CARDWELL, A. COLLINS, E. HOFFMAN, J. SNELL, A. VAHDAT, G. VOELKER, AND J. ZAHORJAN, *Detour: a case for informed internet routing and transport*, IEEE Micro, 19 (1999), pp. 50–59.

[27] J. SHU AND P. VARAIYA, *Pricing network services*, in Proceedings of IEEE INFOCOM 2003, IEEE, 2003.

[28] I. STOICA, R. MORRIS, D. KARGER, F. KAASHOEK, AND H. BALAKRISHNAN, *Chord: A scalable Peer-To-Peer lookup service for internet applications*, in Proceedings of the 2001 ACM SIGCOMM Conference, 2001, pp. 149–160.

[29] V. VISHNUMURTHY, S. CHANDRAKUMAR, AND E. G. SIRER, *Karma: A secure economic framework for peer-to-peer resource sharing*, in Proceedings of Workshop on Economics of Peer-to-Peer Systems, 2003.

[30] W. WANG AND B. LI, *Market-driven bandwidth allocation in selfish overlay networks*, in Proceedings of IEEE INFOCOM 2005, IEEE, March 2005.

[31] B. Y. ZHAO, L. HUANG, J. STRIBLING, S. C. RHEA, A. D. JOSEPH, AND J. D. KUBIATOWICZ, *Tapestry: A global-scale overlay for rapid service deployment*, IEEE Journal on Selected Areas in Communications, (2003). Special Issue on Service Overlay Networks.