Henrique Galperin

Composição de Campos Magnéticos Virtuais com Sistemas de Confiança e Reputação

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Curitiba
2011

Henrique Galperin

Composição de Campos Magnéticos Virtuais com Sistemas de Confiança e Reputação

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Área de Concentração: Sistemas Distribuídos

Orientador: Luiz Augusto de Paula Lima Jr.
Co-orientador: Alcides Calsavara

Curitiba
2011

Galperin, Henrique
Composição de Campos Magnéticos Virtuais com Sistemas de Confiança e Reputação. Curitiba, 2011.

Dissertação - Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática.

1. Campos Magnéticos Virtuais 2. P2P 3. EigenTrust I.Pontifícia Universidade Católica do Paraná. Centro de Ciências Exatas e Tecnologia. Programa de Pós-Graduação em Informática II - t

Sumário

Lista de Figuras

Resumo

Campos Magnéticos Virtuais propõem um novo paradigma para roteamento de mensagens ponto-a-ponto em sistemas distribuídos baseado no conceito de campos magnéticos importado da física. Uma das características das redes magnéticas virtuais é que, com a rede estabilizada (i.e. sem mensagens de controle sendo transmitidas ou recebidas), todas as requisições são direcionadas para o nó denominado pivô, que é aquele que possui a maior força de atração. Considerando que as forças de atração são calculadas em cada nó da rede e devido ao caráter descentralizado do algoritmo proposto, existe a possibilidade de um dos nós ter um comportamento inesperado, alterando arbitrariamente sua força de atração, tornando-se o nó pivô, e atraindo assim para si todas as mensagens da rede sem, no entanto, ter capacidade para tratá-las. Tal comportamento pode gerar um "buraco negro"na rede magnética, tornando o mecanismo inútil na área afetada pelo comportamento do nó malicioso ou defeituoso. Desta forma, propõe-se a utilização de sistemas de confiança e reputação para mitigar os efeitos dos nós que se tornam pivôs e são incapazes de prestar o serviço esperado. Para este fim, optou-se pelo EigenTrust como sistema de confiança e reputação, pois ele provê um mecanismo matematicamente confiável de se obter reputações globais dos nós, e é mais facilmente adaptável ao contexto de redes magnéticas virtuais. Esta dissertação propõe, adicionalmente, a otimização do EigenTrust utilizando campos magnéticos virtuais, além de definir uma metodologia de criação de topologia dinâmica em redes magnéticas virtuais que evita a quebra do grafo em caso de saída de nós da rede. Uma vez estabelecido o sistema de confiança e reputação, são propostos dois modelos de aplicação das reputações. Os resultados das simulações mostram uma redução significativa do recebimento de mensagens por nós com baixa reputação, independente da distribuição de reputações no grafo, apresentando uma solução viável para o problema de "buracos negros"em redes magnéticas virtuais. Além disso, foram introduzidas melhorias no sistema de confiança e reputação EigenTrust com um novo método de estabelecimento de topologia de forma dinâmica em redes magnéticas

virtuais.

Palavras-chave: Campos Magnéticos Virtuais, P2P, EigenTrust, Sistemas de Confiança e Reputação

Capítulo 1

Introdução

1.1 Motivação

Muitos novos desafios na pesquisa de computação expõem uma demanda crescente de aplicações, *middlewares* e paradigmas que exploram e dão suporte ao redirecionamento de mensagens em sistemas distribuídos. Neste contexto um novo paradigma para roteamento de mensagens em sistemas distribuídos ponto-a-ponto baseado no conceito de campos magnéticos importado da física foi proposto (LIMA JR.; CALSAVARA, 2010) (CALSAVARA; LIMA JR., 2010).

O modelo descrito visa englobar situações em que é necessaria a entrega de mensagens para nós específicos de acordo com alguns aspectos não funcionais que dizem respeito à semântica da aplicação. Um exemplo seria uma aplicação que necessita enviar uma mensagem para o nó que pode tratar sua demanda de forma mais eficiente no momento, sem no entanto conhecer a disponibilidade de processamento de todos os nós capazes de tratar a requisição.

A solução desenvolvida envolve a utilização de uma rede *overlay* (representada por um grafo direcionado) sobreposta à rede física para melhor representar a visão da aplicação sobre as relações de "atração"de mensagens entre os nós.

Tendo esta rede *overlay* como base, os autores propõem o conceito de campos magnéticos virtuais, em que cada nó da rede pode agir como um magneto, atraindo mensagens para si com diferentes forças de atração de acordo com a relações da rede *overlay*. As intensidades de atração dos nós são dependentes da semântica da aplicação (no exemplo citado, a disponibilidade de processamento representaria a força de atração) e influenciam seus vizinhos diretos, e, por meio deles, indiretamente seus sucessores no grafo.

O objetivo do mecanismo é fazer com que uma mensagem, não importa por onde ela entre na rede, chegue ao nó com maior força de atração possível de acordo com o grafo de influências magnéticas definido. Para possibilitar tal paradigma, realiza-se a troca de mensagens de controle entre os nós com influência mútua, de forma que cada nó tenha as informações necessárias e suficientes para encaminhar as mensagens ao nó mais forte que o influencie direta ou indiretamente.

Uma das características das redes magnéticas virtuais é que, com a rede estabilizada (i.e. sem mensagens de controle sendo transmitidas ou recebidas), todas as requisições são direcionadas para o nó denominado pivô, que é aquele que possui a maior força de atração. Considerando que as forças de atração são calculadas em cada nó da rede e devido ao caráter descentralizado do algoritmo proposto, existe a possibilidade de um dos nós ter um comportamento inesperado, alterando arbitrariamente sua força de atração, tornando-se o nó pivô, e atraindo assim para si todas as mensagens da rede sem, no entanto, ter capacidade para tratá-las. Tal comportamento pode gerar ou um "buraco negro"na rede magnética, tornando o mecanismo inútil na área afetada pelo comportamento de um único nó.

1.2 Proposta

O objetivo da pesquisa é conceber, em uma rede magnética virtual, um sistema para mitigar os efeitos da manipulação de forças de atração por nós maliciosos ou defeituosos. Um nó malicioso poderia manipular estes valores de duas maneiras diferentes. Por um lado, poderia diminuir sua força de atração para que ele não se torne pivô e não receba nunca carga de trabalho. Ou então, o nó poderia aumentar sua força de atração para se tornar o pivô e atrair todas as mensagens da rede ou pelo menos aqueles enviadas aos nós influenciados direta ou indiretamente por ele.

Para o caso de diminuição artificial da força de atração por um nó malicioso, a ação de contingência seria aumentar a força de atração deste nó sem seu consentimento. No entanto, isto poderia fazer com que ele se torne o pivô e, sendo um possível nó malicioso ou defeituoso, não há garantias que ele trate as mensagens para ele encaminhadas de forma adequada.

Para o caso de aumento artificial da força de atração por um nó malicioso, percebe-se sim a necessidade de uma ação corretiva, pois este nó poderia se tornar o destino de todas as mensagens de dados que entrassem na rede e elas não seriam necessariamente tratadas adequadamente.

Alguns exemplos de aplicações suscetíveis a este tipo de problema são, por exemplo,

o balanceamento de carga e redes de sensores. No balanceamento de carga, o nó com maior força de atração é o nó capaz de absorver mais tarefas. À medida em que ele vai recebendo tarefas, sua ocupação aumenta e sua força de atração tende a diminuir, o que causa uma possível troca de pivô para o nó mais livre no momento. Se um nó, por um defeito ou intencionalmente, não abaixa sua força conforme sua capacidade de processamento diminui, ele se torna um gargalo para toda a rede, podendo inclusive gerar perda de mensagens e a inutilização de toda a área da rede por ele afetada (podendo mesmo ser toda a rede se o grafo que determina as relações de atração for fortemente conexo).

As redes de sensores podem utilizar-se do sistema de redes magnéticas para realizar o roteamento de mensagens até o *sink* pelo caminho com nós com mais bateria. Caso um nó não reduza sua força de atração conforme a redução de bateria, as mensagens continuarão sendo roteadas por ele, causando o descarregamento muito mais rápido deste nó e ruptura prematura nas rotas até o *sink*.

1.3 Contribuição

O presente trabalho de pesquisa produziu três principais contribuições: duas relacionadas principalmente a Redes Magnéticas Virtuais e uma delas surge como uma otimização do sistema de confiança e reputação EigenTrust (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003).

A contribuição principal para Redes Magnéticas Virtuais é uma proposta funcional de uma boa solução para o problema de "buracos negros"em uma rede magnética virtual, quando há um nó malicioso ou defeituoso que artificialmente aumenta sua força de atração, atraindo todas as mensagens de carga de trabalho para si. Esta contribuição se utiliza do sistema de confiança e reputação EigenTrust para ponderar a força de atração informada pelos nós.

A segunda contribuição para Redes Magnéticas Virtuais vem de uma proposta de como se estabelecer uma topologia para geração de planos com entrada e saída de nós dinamicamente, sem, no entanto, haver ruptura do plano em dois ou mais subplanos na rede *overlay*. Esta contribuição se insere na proposta apresentada de otimizar o sistema de confiança e reputação EigenTrust, citado a seguir.

A terceira principal contribuição da pesquisa é a aplicação de Redes Magnéticas Virtuais para substituir o uso de DHTs no sistema de confiança e reputação EigenTrust, com o objetivo de acelerar o processo de busca por *Score Managers*, que são nós responsáveis pela consolidação de reputações de nós específicos na rede. Esta contribuição permite uma abordagem próativa de busca por score managers, trazendo uma otimização

no uso da rede para o EigenTrust.

1.4 Organização

Esta dissertação está organizada da seguinte forma. No Capítulo 2 é apresentado o paradigma de roteamento de mensagens em sistemas distribuídos baseado em campos magnéticos virtuais, incluindo o seu funcionamento básico e os algoritmos distribuídos QuickPath (Seção 2.1) e ShortPath (Seção 2.2) para difusão de mensagens de atualização de forças magnéticas na rede.

Na sequência, no Capítulo 3, são introduzidos conceitos fundamentais sobre sistemas de confiança e reputação e são apresentados os principais modelos distribuídos para estes sistemas encontrados na literatura, a saber: PeerTrust (Seção 3.1), um sistema de confiança e reputação distribuído baseado em redes bayseanas (Seção 3.2), os sistemas CORE e CONFIDANT (Seção 3.3) e finalmente o EigenTrust (Seção 3.4).

No Capítulo 4, um modelo para substituição de DHTs por Redes Magnéticas Virtuais para a escolha de *score managers* é proposto e analisado. O Capítulo 5 examina possibilidades de metodologias de avaliação de nós em uma Rede Magnética Virtual, e na sequência são propostas metodologias para aplicar os valores de reputação para influenciar uma rede magnética virtual para, finalmente, fazer uma análise de simulações comparando estas metodologias e validando os modelos propostos.

O Capítulo 6 conclui o trabalho e apresenta futuras possíveis extensões.

Capítulo 2

Redes Magnéticas Virtuais

Para uma melhor compreensão do funcionamento de redes magnéticas virtuais, consideremos o cenário com quatro nós A, B, C e D, representado na Figura 2.1.

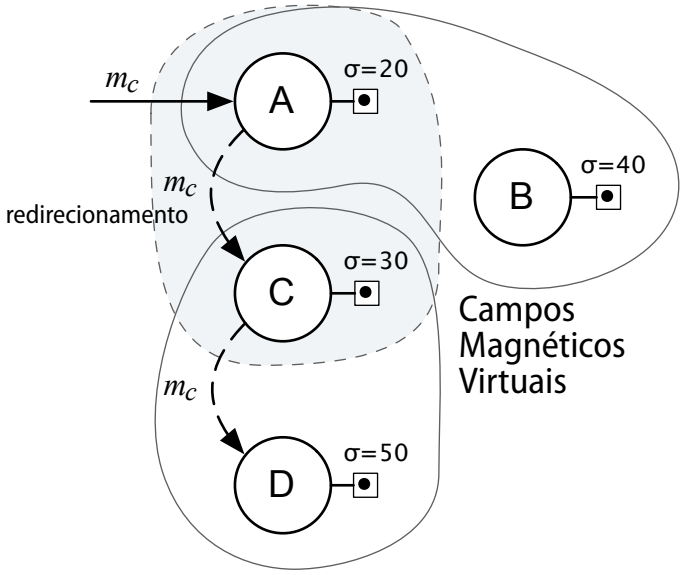


Figura 2.1: Cenário Básico de Campos Magnéticos Virtuais

Neste exemplo, uma mensagem m de um tipo c é enviada inicialmente ao nó A. Supõe-se que todos os nós são potenciais destinatários da mensagem m_c. O nó A é influenciado pelos campos magnéticos dos nós B e C, e o nó C é afetado pelo campo magnético do nó D. Cada nó possui uma força de atração σ. No exemplo, a mensagem m_c, ao chegar em A será redirecionada ao C, pois o nó com maior força que exerce influência (indireta) sobre A é o nó D. Ao chegar em C, a mensagem m_c será finalmente enviada para o nó D, pois é o nó com maior força. O nó D, como não sofre influência de nenhum outro nó, tratará a mensagem.

Em aplicações distribuídas, é comum a utilização de uma rede lógica estruturada sobre a rede física, para satisfazer os requisitos de topologia orientados a fatores dinâmicos relacionados à semântica da aplicação. Estas redes de sobreposição(*overlay*) representam melhor a visão da aplicação sobre os nós. A Figura 2.2 demonstra o uso de tais redes, em que cada plano apresentado representa uma classe magnética sobre a topologia física. As conexões entre nós em uma mesma classe (i.e. mesmo plano) são direcionais, o que permite influências sem mutualidade obrigatória.

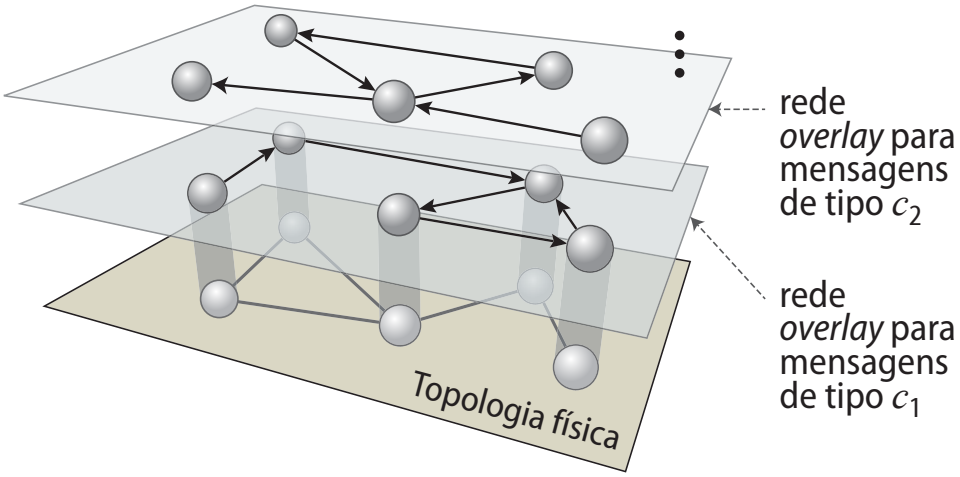


Figura 2.2: Planos Magnéticos em Redes *Overlay*

Para realizar atualizações e propagações dos valores de força de atração dos nós, foram propostos dois algoritmos diferentes: o QuickPath (LIMA JR.; CALSAVARA, 2010), que busca rotas com menor tempo de entrega de mensagens e o ShortPath (CALSAVARA; LIMA JR., 2010), que busca rotas com o menor caminho em saltos para a entrega de mensagens. Estes algoritmos são descritos na sequência.

2.1 QuickPath

Inicialmente, para a correta definição do algoritmo QuickPath, alguns conceitos básicos devem ser assumidos ou definidos:

- Cada nó é representado por um identificador i único;
- Cada nó possui uma lista dos nós vizinhos diretamente influenciados por ele e uma tabela de nós cujos campos magnéticos de uma determinada classe c afetam i, chamada Tabela de Campos Magnéticos (MFT_c);

- Cada entrada de MFT_c é composta por origem, sendo o identificador do nó que o influencia; pivô, sendo o identificador do nó mais forte (direta ou indiretamente); força, sendo a força do pivô;
- O grafo representando as influências magnéticas para uma determinada classe c é uma rede *overlay* chamada de Grafo de Vizinhança (NG_c).

A Figura 2.3 mostra um exemplo de um NG para uma determinada classe (omitida para facilitar a compreensão) e mostra a MFT de cada nó.

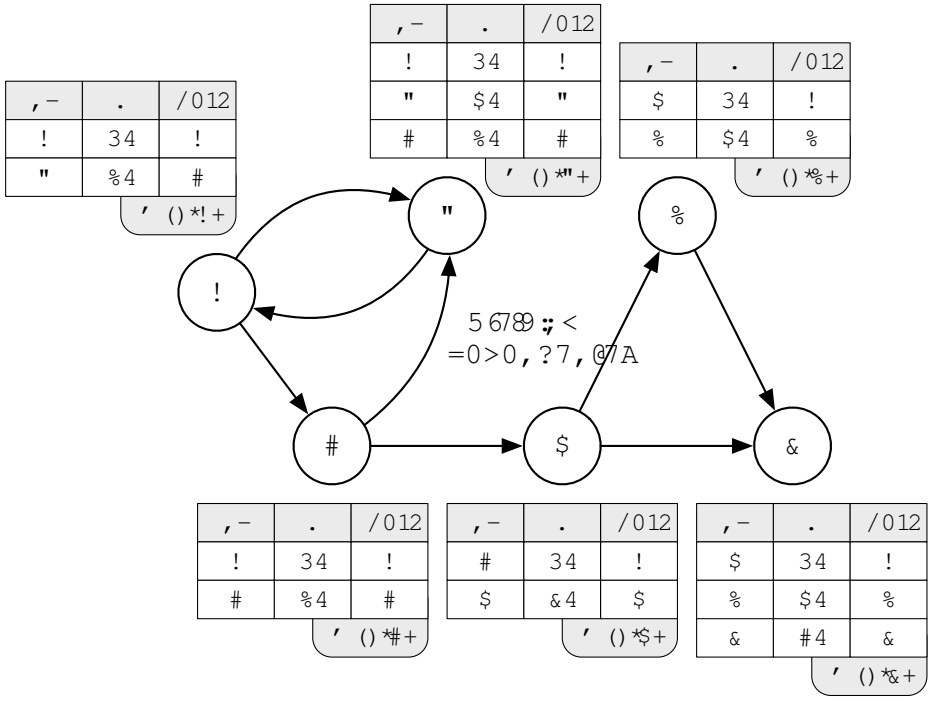


Figura 2.3: Exemplo de Grafo de Vizinhança (NG)

O algoritmo QuickPath parte do seguinte princípio: mensagens de propagação somente são disparadas por eventos que modifiquem a força de atração do nó mais forte ou modificam o pivô percebido por um nó.

Quando esta condição for satisfeita em um determinado nó, ele propaga uma mensagem de controle informando a alteração para todos os seus nós vizinhos. Pode ocorrer o caso de uma mesma mensagem de propagação chegar mais de uma vez em um nó. Neste caso, esta mensagem não será propagada, pois não irá satisfazer a regra citada, o que elimina o risco de mensagens cíclicas na rede. Esta técnica faz com que o caminho mais rápido para que a mensagem de propagação chegue ao seu destino seja também utilizado para as mensagens da aplicação.

Na mensagem de propagação, além da identificação do nó que está enviando a mensagem, do novo nó pivô e da força de atração do novo pivô, ainda são incluídos a força de atração do nó que está enviando a mensagem e o nó e sua respectiva força de atração para o nó com segunda maior força, além de um identificador do evento original que iniciou este ciclo de propagações, usado para *debug*, *tracing* e otimizações. Tendo estas informações, ao receber uma mensagem deste tipo, caso a informação do pivô já tenha sido atualizada por outra mensagem de outro nó, utiliza-se a informação do nó com segunda maior força para atualizar a linha da tabela para o nó de origem. Caso esta informação também seja redundante, utiliza-se as informações do próprio nó de origem. Este modelo garante que caso um nó pivô possa magnetizar outro diretamente, este caminho direto será sempre usado pelas mensagens da aplicação.

As restrições de que o canal de comunicação deve obedecer uma política FIFO; de que internamente, se um nó recebe mensagens em uma determinada ordem, as mensagens que este recebimento gera devem seguir a mesma ordem de recebimento, podem ser eliminadas adicionando-se uma nova coluna na MFT contendo a versão da informação.

Uma linha da tabela é atualizada somente se a versão da mensagem recebida for maior que a versão da informação já constante na tabela para a respectiva linha.

2.2 ShortPath

O algoritmo ShortPath, por outro lado, utiliza-se de uma nomenclatura diferente e novas definições de conceitos:

$F(i)$ é a força de atração de um nó i;

$T(i)$ é a coleção de nós magnetizados por um nó i diretamente;

$S(i)$ é a coleção de nós que magnetizam um nó i diretamente;

$T^*(i)$ é a coleção de nós magnetizados por um nó i direta ou indiretamente;

$S^*(i)$ é a coleção de nós que magnetizam um nó i direta ou indiretamente;

$P^*(i)$ é o nó mais forte de $S^*(i)$, logo ele é o nó pivô;

$P_k(i)$ é o pivô de k na visão de i, definido para cada nó em $S(i)$, ou seja, normalmente $P^*(k)$ será igual a $P_k(i)$;

$K(i)$ é a coleção de nós conhecidos que magnetizam um nó i direta ou indiretamente, ou seja é uma subcoleção de $S^*(i)$, pois nem todos os nós que magnetizam i indiretamente são necessariamente conhecidos;

$M(i)$ é o nó que pertence a $S(i)$ que possui o pivô com maior força. É utilizada para o roteamento.

Neste algoritmo, dois tipos de mensagens são trocadas: mensagens de troca de força e mensagens de troca de pivô. A mensagem de troca de força tem o seguinte conteúdo:

i é o identificador do nó que enviou a mensagem;

j é o identificador do nó de destino da mensagem;

s é o identificador do nó que que o causador da mensagem de troca de força;

$F'(s)$ é a nova força de s;

o *timestamp* correspondente ao tempo local em s quando sua força foi alterada;

a distância entre s e j referente à rede magnética virtual (usada para determinar a menor distância caso dois caminhos existam, e também para detecção de ciclos na rede).

A mensagem de troca de pivô tem a seguinte estrutura:

i é o identificador do nó que descobriu que há uma troca de pivô;

j é o identificador do nó de destino da mensagem;

p é o identificador do nó que é o novo pivô;

o *timestamp* correspondente ao tempo local em i quando ele descobriu que p é o novo pivô;

$F'(p)$ é a força de p quando ele se tornou o novo pivô;

o *timestamp* correspondente ao tempo local em p quando sua força mudou para $F'(p)$;

a distância entre p e j referente à rede magnética virtual (usada para determinar a menor distância caso dois caminhos existam, e também para detecção de ciclos na rede).

Todos os nós devem estar aptos a receber os dois tipos de mensagens. Elas são tratadas conforme descrito a seguir:

Para a mensagem de troca de força:

1. se a mudança de força notificada por m é relevante de acordo com timestamps em m e $K(j)$ então
   (a) registre em $K(j)$ todos os dados sobre s contidos em m
   (b) se a força de s decaiu então
      i. envie uma mensagem de mudança de força para todos os nós em $T(j)$ para notificar sobre s
      ii. se s se tornar $S^*(j)$ então
         A. atualize $S^*(j)$ e $M(j)$ de acordo com os dados em $S(j)$
         B. se qualquer dado relativo a $S^*(j)$ mudou, então envie uma mensagem de mudança de pivô para todos os nós em $T(j)$ para notificar sobre $S^*(j)$

E para a mensagem de troca de pivô:

1. se a mudança de pivô de i notificada por m é relevante de acordo com timestamps em m e $S(j)$ então
   (a) registre em $S(j)$ todos os dados sobre i e p contidos em m
   (b) se ou a força de p notificada por m é legada de acordo com os timestamps em m e em $K(j)$ ou a distância de p à j notificada por m é maior que a respectiva distância registrada em $K(j)$, significa que há um loop infinito de mensagens, então
      i. marque i como obsoleto em $S(j)$
      ii. se não se a força de p notificada por m é relevante de acordo com os timestamps em m e $K(j)$ então
         A. registre em $K(j)$ todos os dados sobre p contidos em m
         B. se a força de p decaiu, então envie uma mensagem de mudança de força para todos os nós em $T(j)$ para notificar sobre p
   (c) atualize $S^*(j)$ e $M(j)$ de acordo com os dados em $S(j)$
   (d) se qualquer dado relativo a $S^*(j)$ mudou, então envie uma mensagem de mudança de pivô para todos os nós em $T(j)$ para notificar sobre $S^*(j)$

2.3 Conclusão

Neste capítulo foi apresentado o conceito de Redes Magnéticas virtuais, assim como seu funcionamento básico. Na sequência, dois algoritmos de Redes Magnéticas virtuais

foram detalhados. O primeiro deles, o QuickPath propõe um algoritmo de propagação que gera o caminho mais rápido para que a mensagem chegue ao seu destino. Já o algoritmo ShortPath gera um caminho com menor número de saltos possíveis para que uma mensagem seja roteada ao destino.

Para as experiências realizadas, utilizou-se o algoritmo QuickPath. Apesar do ShortPath ser também uma escolha viável, optou-se pelo QuickPath pois esta opção possui um simulador estável e com a colaboração e suporte facilitado, por ter sido desenvolvido pelo orientador desta pesquisa. A escolha do algoritmo a princípio não influencia a aplicação de reputações na rede magnética virtual, uma vez que este mecanismo age principalmente no roteamento de mensagens com carga de trabalho, de forma relativamente independente do mecanismo de escolha de rotas, sendo elas pelo caminho mais rápido (QuickPath) ou pelo caminho mais curto (ShortPath).

Capítulo 3

Sistemas de Confiança e Reputação

O primeiro passo para se compreender sistemas de confiança e reputação é entender o que exatamente, na literatura técnica, significam as palavras "confiança"e "reputação". (JøSANG; ISMAIL; BOYD, 2007) possui uma definição bem clara destes conceitos: inicialmente a definição de confiança é subdividida em duas categorias (apesar de na maioria das vezes serem consideradas de maneira única).

O primeiro conceito de confiança, definido originalmente em (GAMBETTA, 1988), pode ser traduzido como confiança simples (*Reliability Trust* em inglês), define que confiança é a probabilidade subjetiva na qual um indivíduo A espera que outro indivíduo B execute uma determinada ação da qual ele dependa. Este conceito traz uma definição simplista demais. Ter uma confiança elevada em uma pessoa não é suficiente para entrar em uma relação de dependência com ela. (CASTELFRANCHI; FALCONE, 2002) exemplifica esta limitação com o caso em que uma falha em uma dependência cause tanto dano que mesmo com confiança no outro envolvido (probabilidade de falha muito baixo), não se deseje assumir o risco.

Em (MCKNIGHT; CHERVANY, 2001) é proposto o segundo conceito de confiança: a confiança de decisão (*Decision Trust* em inglês). Ele define que confiança é a medida em que uma das partes está disposta a depender de algo ou alguém em uma situação dada com percepção de relativa segurança, apesar da possibilidade de consequências negativas. Esta definição considera não só o nível de confiança no confiado, mas também considera o dano que uma possível falha pode ocasionar.

Reputação é um conceito complementar ao conceito de confiança, pode-se definir reputação como sendo, segundo (FREEMAN, 1979) e (MARSDEN; LIN, 1982), o que é geralmente dito ou se acredita sobre o caráter ou posicionamento de uma pessoa. As diferenças entre confiança e reputação podem ser claramente ilustradas com as seguintes sentenças: "Eu confio em você porque você tem boa reputação"e "Eu confio em você apesar de sua

má reputação".

Tendo estas definições em mente, é possível ainda dividir sistemas de confiança e reputação em duas categorias: as que possuem um serviço centralizado para autenticar e armazenar os valores de reputação e os sistemas distribuídos. Sistemas com serviço centralizado são amplamente aplicados e pesquisados. O comércio eletrônico é um dos principais usuários destes sistemas. Empresas como EBay, Mercado Livre e Amazon utilizam sistemas de reputação para avaliar o desempenho de vendedores. Forums e sites de clipping colaborativo na internet como Slashdot e Digg aplicam a reputação para classificar os usuários que colaboram de forma positiva ou negativa para a comunidade de usuários. O Google e seu algoritmo PageRank, descrito em (BRIN et al., 1998), utiliza o link de outros sites para contabilizar sua reputação.

Como redes magnéticas virtuais são redes distribuídas, estudou-se principalmente sistemas de confiança e reputação distribuídos, como sistemas voltados a redes ponto-a-ponto e ad-hoc, que por sua vez exigem um grau de complexidade maior que os com serviço centralizado, pois não há entidades que possam servir como uma terceira entidade confiável. O principal desafio de construir estes mecanismos de reputação e confiança distribuídos é encontrar uma maneira efetiva de impedir vários comportamentos maliciosos como, por exemplo, um nó na rede prover um parecer falso sobre outro nó. Segundo (XIONG; LIU, 2004), ainda é um desafio construir um sistema de confiança e reputação distribuído que seja eficiente, escalável e seguro, e ainda há a necessidade de métodos de avaliação experimental de um modelo de confiança e reputação em termos de efetividade e benefícios.

3.1 PeerTrust

No artigo (XIONG; LIU, 2004) os autores propõem o sistema PeerTrust. Inicialmente é importante citar em que fatores o PeerTrust se baseia para calcular a confiança de um elemento na rede:

1. A avaliação recebida de outros nós na rede;
2. O escopo da avaliação, como por exemplo o número total de transações que o nó avaliado teve com outros nós;
3. O fator de credibilidade da fonte da avaliação;
4. O fator de contexto da transação para diferenciar transações críticas de transações com menor importância;

5. O fator contexto da comunidade, para tratar características específicas de cada comunidade, como por exemplo nós com certificação digital reconhecida poderiam ter este índice mais elevado.

Na sequência os autores mostram como reunir estes fatores matematicamente, levando em consideração dois fatores α e β que representam, respectivamente, o peso para as avaliações recebidas de outros nós e o peso para os fatores de contexto da comunidade. Ajustando estes fatores, pode-se configurar o sistema para que objetivos específicos sejam alcançados com o PeerTrust.

Para o cálculo da confiança em um nó, são propostas duas estratégias, e para ambas são consideradas as opções de coleta dinâmica de informações de reputação ou então o cache destas informações para uso futuro. Para resolver problemas de variação de qualidade no tempo, é proposta a utilização de duas janelas de tempo diferentes para o cálculo da confiança, uma longa e uma curta. Se a curta tiver um decaimento de confiança acima de um limite estabelecido sobre a longa, o valor de confiança da menor janela será utilizado, caso contrário, será utilizado o da maior janela. Desta forma este comportamento dinâmico é levado em conta. Para garantir a segurança de transmissão de dados de reputação o artigo propõe a utilização de um esquema baseado em PKI e replicação.

3.2 Sistema de Confiança e Reputação Baseado em Redes Bayesianas

O artigo (WANG; VASSILEVA, 2003) propõe um modelo de confiança e reputação baseado em redes Bayesianas. Ele se baseia na ideia de que nós necessitam desenvolver confiança em diferentes aspectos sobre as capacidades de outro nó. Dependendo da situação, um nó pode confiar ou não em outro. Um exemplo seria que alguém poderia confiar em outra pessoa para consertar seu carro, mas provavelmente não confiaria nela para ser seu médico. Este exemplo seria o que o artigo citado nomeia de especificidade ao contexto. Outro conceito apresentado é a confiança multi-facetada, em que por exemplo, para consertar meu carro, outros fatores como qualidade do serviço, preço, etc. devem influenciar a confiança final. Um terceiro conceito é a dinamicidade da confiança, em que além de crescer ou diminuir com experiências, a confiança também decai com o tempo. O artigo mostra que o uso do contexto de forma a influenciar a confiança para cada tipo de transação gera um ganho para o sistema como um todo.

3.3 CORE e CONFIDANT

Já o artigo (YAU; MITCHELL, 2003) é voltado a sistemas de reputação em redes móveis ad-hoc (MANET). Ele apresenta dois modelos de sistemas de reputação: o CORE e o CONFIDANT, resumidos na sequência.

O CORE define três tipos de reputação que, combinados, geram um valor global de reputação para um membro da comunidade. Todo cálculo é normalizado para que os valores se mantenham entre -1 (ruim) a 1 (bom), onde 0 significa que não há observações suficientes. Os três tipos de reputação são: subjetiva, que é calculada localmente, com ênfase em comportamentos passados, para diminuir a influência de comportamentos esporadicamente bons; a reputação indireta, em que um nó informa sua percepção de outro a um terceiro, em que somente se utiliza valores positivos de reputação, para evitar que um nó malicioso tente realizar um ataque de negação de serviço; e a reputação funcional, onde cada funcionalidade é ponderada de acordo com sua importância.

Nele existem três casos em que a tabela de reputações é atualizada: na interação direta com um nó, quando há uma distribuição global de reputações de um nó ou quando uma reputação é gradualmente reduzida com o tempo até que chegue a zero.

Quando um nó A, com boa reputação, é solicitado para um serviço pelo nó B, que tem má reputação, o nó A pode se negar a cooperar. Ao fazer isto, ele deve enviar uma mensagem a todos os nós na rede sobre a negação de serviço. Os nós que não concordam com esta negação (tem reputação positiva para B) então reduzem a reputação de A.

O protocolo CONFIDANT, por outro lado, se baseia no monitoramento de pacotes que passam pelo nó. Caso seja detectada alguma atividade suspeita, uma mensagem de alarme pode ser enviada para todos os nós em uma lista de "amigos". Ao receber uma mensagem de alarme, um nó verifica se a origem da mensagem é confiável, e pondera seu peso. Ao atingir um limite, o nó em questão pode ser colocado em uma lista negra e só sai dela por expiração de tempo. Estas informações são então utilizadas para o cálculo de roteamento de mensagens na rede ad-hoc.

Os autores do artigo fazem uma análise comparativa das duas técnicas: enquanto o CORE utiliza reputações negativas e positivas, o CONFIDANT utiliza somente reputações negativas. No CORE, se um nó tem boa reputação e temporariamente não é capaz de executar uma operação, ele não será punido severamente, ao contrário do CONFIDANT. Esta abordagem é, no entanto, vulnerável a um ataque de variação de qualidade no tempo.

Existe ainda uma outra consideração dos autores, que cita que um nó que construa boa reputação pode virar um gargalo do serviço, devido à alta de demanda, o que poderia levar a nós agirem de forma ruim para baixar um pouco sua reputação. Isto poderia ser

mitigado colocando mais peso em comportamentos ruins do que bons, desta forma um comportamento indesejado iria ter uma influência muito maior.

3.4 EigenTrust

O artigo (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003) apresenta um sistema de reputação distribuído para redes ponto-a-ponto. Ele se baseia na ideia de que cada nó na rede deve possuir um valor de reputação global, que reflete a experiência que todos os nós na rede tiveram com um determinado nó i. O cálculo da confiança local é feita através da contagem de pontos de um nó, sendo que para cada transação positiva, é somado um ponto, e para cada negativa é subtraído um ponto. Este valor é então normalizado entre 0 e 1. A reputação global de cada nó i é dada pelos valores locais de confiança atribuídos ao nó i por outros nós, ponderados pelas reputações globais dos nós avaliadores.

O modelo propõe a utilização de DHTs para mapear os nós da rede, usando hashes sucessivos de um identificador único do nó alvo, como o IP mais a porta TCP como chave (utiliza-se a porta pois pode haver mais de um plano por nó físico na rede). Desta maneira, o resultado destes sucessivos hashes apontariam para diferentes espaços na DHT, e os nós responsáveis por estes espaços seriam escolhidos como *score managers*, responsáveis pela consolidação da reputação do nó alvo. Como os *score managers* são escolhidos aleatoriamente, não há informação de quem está sendo avaliado e múltiplos *score managers* são usados para calcular e armazenar a pontuação de um nó, é garantido o anonimato, aleatoriedade e redundância.

Mais detalhes dos mecanismos internos deste sistema são descritos no desenvolvimento desta dissertação, juntamente com propostas de melhoria do mesmo.

3.5 Conclusão

Neste capítulo foram apresentados os conceitos básicos de sistemas de confiança e reputação, foi realizada uma introdução relativa a sistemas de reputação distribuídos. Na sequência foram apresentados diversos sistemas de confiança e reputação e finalmente foi apresentado o sistema de confiança e reputação utilizado neste trabalho: o EigenTrust, apresentando suas principais características e vantagens.

Optou-se pelo EigenTrust como escolha de sistema de confiança e reputação pois ele provê um mecanismo matematicamente confiável de se obter reputações globais dos nós. Nos outros sistemas pesquisados a visão de reputação de cada nó é diferente. Este

fator do EigenTrust permite uma maior uniformidade quando os valores de reputação são aplicados à rede magnética virtual, o que garante maior estabilidade no roteamento de mensagens e propagação de forças de atração.

Capítulo 4

Otimização do EigenTrust Usando Redes Magnéticas Virtuais

No EigenTrust, o valor de confiança de cada nó é calculado por uma coleção de outros nós chamados *Score Managers*. Os *Score Managers* de cada nó são aleatoriamente escolhidos através de aplicações sucessivas de uma função *hash* em um identificador exclusivo do nó, como o endereço IP e a porta TCP, resultando em pontos em um espaço de uma DHT (a DHT proposta originalmente no EigenTrust é a CAN (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003)). Os nós que ocuparem estes espaços serão os *Score Managers* do respectivo nó.

Embora o EigenTrust, na sua especificação original, use uma DHT para a seleção de *Score Managers*, sugerimos que este mecanismo possa ser substituído por uma Rede Magnética Virtual, diminuindo a carga da rede nas operações de pesquisa de *Score Managers*.

A ideia principal é utilizar um plano virtual magnético por *Score Manager*. O nó pivô em um plano será o *Score Manager* selecionado. As forças magnéticas de todos os nós devem ser aleatórias e auditáveis por qualquer outro nó no plano, para garantir que o *Score Manager* escolhido é realmente aleatório e sua escolha não foi manipulada.

Dado que a reputação de cada nó pode ser avaliado por s *Score Managers* (normalmente um valor global constante) e sabendo que cada *Score Manager* requer um plano virtual magnético individual, teremos $s \times N$ (onde N é o número de nós na rede) planos. Visando reduzir este número, é possível agrupar nós, permitindo que eles compartilhem o mesmo conjunto de *Score Managers*.

4.1 Motivação

A principal motivação para a substituição de DHTs por Redes Magnéticas Virtuais é que esta última tem uma maneira pró-ativa de manipulação de roteamento, enquanto DHTs agem de maneira reativa. Isto significa que quando um nó precisa saber quem é o *Score Manager* de um outro nó, ao usar um DHT, ele precisará fazer uma pesquisa na rede, entrando em contato com diversos nós para obter a resposta. Isso não acontece quando se usa Redes Magnéticas Virtuais, já que a informação é, de uma forma pró-ativa, conhecida por todos.

Mesmo tendo um algoritmo pró-ativo, mostraremos nas próximas seções que este comportamento não causa uma sobrecarga significativa na rede na entrada ou saída de um nó da rede, uma vez que só haverá um grande número de mensagens trocadas quando o *Score Manager* for alterado.

A utilização de Redes Magnéticas Virtuais faz com que o EigenTrust seja muito mais eficiente em suas operações mais comuns, como a pesquisa de um *Score Manager* e na entrada ou saída de um nó que não seja o *Score Manager*, o custo adicional desta mudança ocorre apenas nas operações menos usadas, como a entrada ou saída de um *Score Manager*.

4.2 Estabelecimento e Manutenção de Topologia de Rede Magnética Virtual

Para substituir DHTs por Redes Magnéticas Virtuais no EigenTrust, é preciso definir como os nós são organizados nos planos magnéticos virtuais. Duas categorias principais de topologia dos planos podem ser identificadas: a topologia estática, onde não existe entrada ou saída de nós, e a topologia dinâmica, com nós entrando e saindo do plano a qualquer momento.

No cenário de topologia estática, uma boa opção é construir os planos como *Small World* (WATTS; STROGATZ, 1998) com um número reduzido de arestas, mas, ao mesmo tempo, sem aumentar o número médio de saltos entre os nós. Outras técnicas podem ainda ser usadas, incluindo a reprodução da topologia física subjacente.

Ao considerar uma topologia dinâmica, há sempre o risco de, quando há saída de nós da rede, desconectar o plano magnético virtual. Mesmo estas desconexões não impededindo o funcionamento do EigenTrust. Elas podem sim comprometer seu desempenho, considerando que cada plano separado teria seu próprio *Score Manager* com

informações replicadas desnecessariamente. Se esta situação não é evitada ou minimizada, a segmentação de planos tende a crescer ao longo do tempo, resultando em um número indesejável de *Score Managers*. Sendo assim, propomos um modelo para evitar a segmentação do plano em uma topologia de rede dinâmica.

Para se conectar à rede, um nó i só precisa conhecer um nó de *bootstrap*. É desejável, no entanto, que i se conecte também a pelo menos outro(s) nó(s) escolhido(s) aleatoriamente, a fim de reduzir a chance de divisão do plano em caso de desconexões posteriores. Se i é o pivô novo do plano, então esta informação é divulgada através de um dos algoritmos de propagação propostos para Redes Magnéticas Virtuais, como (LIMA JR.; CALSAVARA, 2010) ou (CALSAVARA; LIMA JR., 2010).

Para tratar o caso de saída de nós da rede, assume-se que cada nó é capaz de detectar a desconexão de um vizinho direto, seja através de *pooling* ou outro método. Existem duas categorias de nós que podem deixar a rede: pivôs e "nós regulares"(ou seja, não pivôs). Se um nó regular deixa o plano magnético, então a rede será afetada somente se este nó é parte da rota de outro nó regular até o pivô.

Quando um nó regular i detecta que um dos seus vizinhos diretos i_n deixou a rede, ele deve verificar se o nó que saiu faz parte de sua rota para o pivô. Se não fizer, então nada precisa ser feito. Se, no entanto, i_n faz parte do caminho para o pivô, então i deve se conectar diretamente ao pivô, a fim de manter a rede coesa e para restaurar sua conectividade com o pivô. A conexão direta com o pivô é sempre possível pois cada nó conhece a identidade do pivô. Uma vez que, neste caso, o pivô não mudou, todas as rotas preexistente ainda serão válidas, e nenhuma mudança de força de atração precisa ser propagada. Este processo é ilustrado na Figura 4.1, onde o nó 2 deixa o plano e força o nó 3 a estabelecer uma nova conexão direta com o pivô.

Por outro lado, se o nó que está saindo é o pivô, então um pivô secundário (ou seja, o nó com a a segunda maior força de atração do plano) se torna o novo pivô e sua força de atração é propagada para todos nós no plano. Se ele deixa a rede antes do pivô em si, então o mesmo procedimento usado quando um nó regular deixa o plano é realizado, e então um novo pivô secundário deve ser escolhido, usando os mecanismos existentes de propagação.

Portanto, quando um pivô sai da rede, o pivô secundário torna-se o pivô, e todos os vizinhos do pivô que deixou a rede verificam se eles ainda têm uma rota ativa até o novo pivô. Se não tiverem, eles devem criar uma conexão diretamente ao novo pivô. Este procedimento garante a coesão da topologia de plano. Como os pivôs deste plano foram alterados, todas as forças de atração precisam ser propagadas, começando pelos nós que perderam a conexão direta com o pivô anterior. Naturalmente, o plano magnético vai

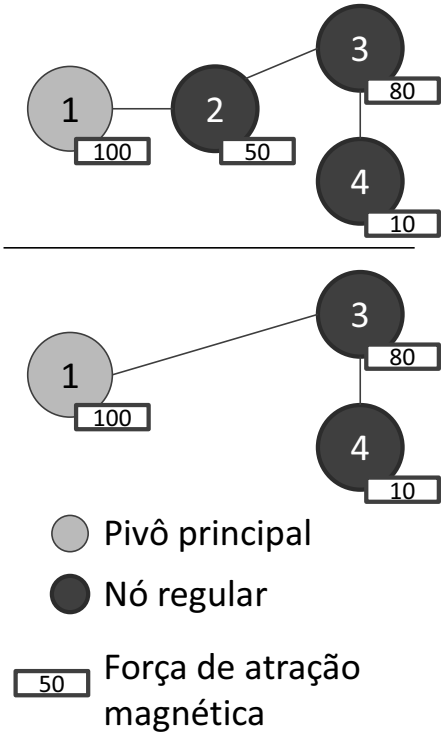


Figura 4.1: Saída de um nó regular que pertence a uma rota até o pivô.

eleger um novo pivô secundário e será atualizado com o novo pivô, usando os algoritmos tradicionais de propagação em Redes Magnéticas Virtuais.

A Figura 4.2 retrata um cenário em que o pivô (nó 3) sai da rede. Depois disso, o nó 2 se conecta ao pivô secundário (nó 4), que vai se tornar o novo pivô e, em seguida, um pivô secundário é eleito (nó 1, neste exemplo).

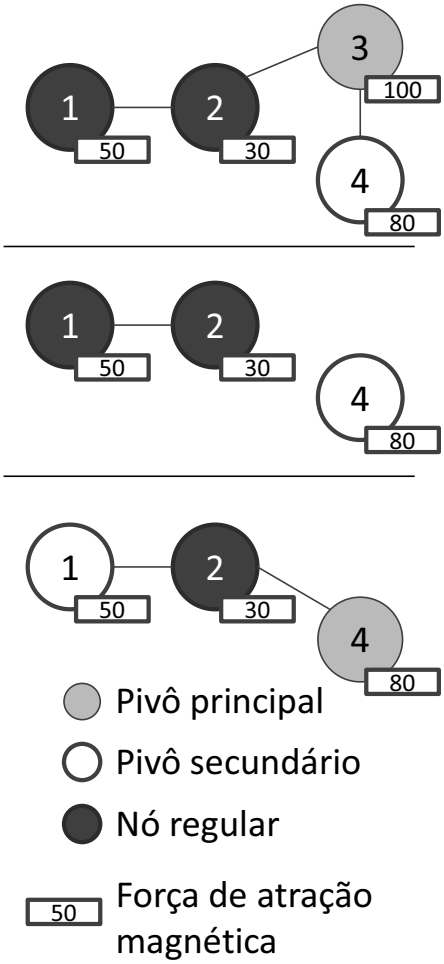


Figura 4.2: Saída de pivô.

4.3 Cálculo de Forças de Atração

Uma vez que a topologia da rede magnética foi estabelecida, o próximo passo consiste em definir um método para atribuir forças de atração para cada nó. Considerando que esta força de atração será utilizada para selecionar o *Score Manager* para um determinado nó (ou grupo de nós), o método deve gerar valores de força de atração que sejam únicos e aleatórios dentro de um plano e diferentes para cada nó em múltiplos planos.

Para garantir o anonimato e aleatoriedade requeridos pelo EigenTrust, definimos a força de atração $F(i)$ de um dado nó i de acordo com a Equação 4.1.

$$F(i) = H(H(I(t)) + I(i) + k) \tag{4.1}$$

Sendo,

H uma função de hash conhecida e confiável, como SHA1 (FIPS, 2002);

$I(i)$ um identificador único do nó i;

t o nó do qual a reputação é calculada pelo *score manager*;

k um número natural usado para distinguir *score managers* pertencentes a diferentes planos de atração. Por exemplo, se existem três *score managers* por nó (ou grupo de nós), então k variará de 0 a 2.

A Equação 4.1 gera resultados aleatórios devido à função hash H. Ela também garante o anonimato ao usar $H(I(t))$ no lugar de $I(t)$ diretamente, e ainda minimiza a probabilidade de existir forças iguais para diferentes nós dentro do mesmo plano, uma vez que $I(n)$ é distinta para cada n. Além disso, a probabilidade um nó de ter o mesmo *score manager* em diferentes planos é mínima, pois k tem diferentes valores em cada plano.

É possível observar também que todos os parâmetros da Equação 4.1 são conhecidos de todos nós no plano magnético. Como consequência, é praticamente impossível para um nó malicioso forjar uma força de atração ou corromper mensagens de propagação de força.

4.4 Agrupamento de Nós

Da Equação 4.1, pode-se observar que planos magnéticos podem ter algumas variáveis idênticas para todos os nós no plano, sendo elas representadas pelo par $[H(I(t)), k]$. Portanto, se multiplicarmos o número de $H(I(t))$ existentes pelo número de planos (ou seja, *score managers*) por nó, obtemos a quantidade total de planos na rede.

Pode-se observar que se houver um $H(I(t))$ diferente para cada t (sendo t um nó na rede), o número total de planos pode ser muito alto, e poderia trazer sobrecarga para a rede. Para reduzir o número de planos, vários nós podem ser agrupados de forma que utilizem o mesmo plano e os mesmos *score managers*. Isto pode ser feito através da realização da divisão inteira de $H(I(t))$ por um constante g, para cada nó t. Nós que apresentam o mesmo resultado irão pertencer ao mesmo grupo, e $H(I(t))/g$ irá substituir $H(I(t))$ na Equação 4.1. Por exemplo, se existem três nós i, j e k em uma rede, e $H(I(i)) = 20$, $H(I(j)) = 24$ e $H(I(k)) = 35$, então, se $g = 10$, os nós i e j passarão a pertencer ao mesmo grupo (uma vez que $H(I(i))/g = H(I(j))/g = 2$) e, portanto, eles irão compartilhar os mesmos *score managers*. Esta estratégia reduz o risco de manipulação, pela criação de grupos aleatórios.

Deve-se notar que é importante escolher a constante g de acordo com o número esperado de nós na rede e a magnitude de H. Por exemplo, se há apenas alguns nós na rede e H produz números de grande magnitude, é desejável usar um valor alto para g, de modo a aumentar a probabilidade de dois nós pertencem ao mesmo grupo.

4.5 Propagação de Forças de Atração

Considerando que a força de atração de todos os nós no plano magnético pode ser calculada por qualquer outro nó, é possível simplificar o algoritmo de propagação força. É possível propagar apenas o identificador dos nós, removendo a força de atração da tupla propagada, e calcular as forças de atração nó localmente.

4.6 Comparação com Solução Existente

Uma comparação entre as redes magnéticas virtuais e DHTs como abordagens para implementar um sistema para determinar os *score managers* no EigenTrust pode ser feita pela avaliação da utilização de recursos da rede em ambos os casos. Os seguintes eventos devem ser levados em conta para fazer uma comparação justa: a entrada de um nó na rede, a saída de um nó da rede, e a seleção dos *score managers* para um nó arbitrário.

Se somente a seleção do *score manager* for considerada, é possível notar que a abordagem baseada em redes de campo magnético apresenta uma clara vantagem, pois todos os nós conhecem o novo pivô o tempo todo e, consequentemente, nenhuma mensagem é necessária para a descoberta do *score manager*, enquanto na abordagem baseada em DHTs, a navegação através da rede é necessária, a fim de descobrir qual nó ocupa a posição correspondente ao *score manager*, causando assim diversas trocas de mensagens.

No caso de entrada e saída de nós, há apenas dois casos que podem causar algum impacto no desempenho para a abordagem baseada em redes magnéticas virtuais. Em primeiro lugar, se um nó que entra ou sai da rede é o *score manager*, haverá uma alguma degradação desempenho, já que o processo de atualização do novo pivô será acionado (ver Seção 4.2). Em todos os outros casos, as consequências não são relevantes. Por outro lado, se por exemplo CAN é empregada, o impacto é quase sempre baixo, já que na maioria dos casos, somente os nós vizinhos precisam ser notificados, para que seja feita a divisão da área existente (quando um nó entra na rede) ou ocupar uma área recém liberada (quando um nó deixa a rede), se um *take-over* não for necessário (CLAESSENS; PRENEEL; VANDEWALLE, 2003). Assim, na abordagem baseada em DHTs, o desempenho é melhor do que na abordagem baseada em campos magnéticos virtuais nos casos em que o nó que entra ou sai da rede é o *score manager*. No entanto, quanto maior for a rede, menor são as chances para que isso aconteça.

Portanto, assumindo que a entrada e saída de *score managers* acontecem em uma taxa muito menor do que a busca por *score managers*, a abordagem baseada em redes magnéticas virtuais terá um desempenho global melhor do que a abordagem baseada em

DHTs.

Os custos de entrada e saída no nó de redes magnéticas virtuais e no CAN são analisadas nas seções seguintes.

4.6.1 Análise de Custo de Troca de Mensagens em Redes Magnéticas Virtuais

Considerando as seguintes variáveis:

N o número de nós em um plano

E o número de arestas (conexões entre dois nós) no plano, assumindo que todas as arestas são bidirecionais;

Ei o número de arestas criadas por um nó ao entrar na rede;

Ce o custo de criação de uma nova aresta bidirecional;

Ea o número médio de arestas por nó.

A probabilidade (P) de que um nó que esteja entrando ou saindo do plano magnético seja um pivô primário ou secundário pode ser definida pela Equação 4.2.

$$P = \frac{2}{N} \tag{4.2}$$

Se há uma mudança de pivô, o número de mensagens necessárias para selecionar um novo pivô é dado pela Equação 4.3 (custo de propagação).

$$Cp = 2 \times E - N + 1 \tag{4.3}$$

Baseado na Equação 4.3, é possível calcular o custo médio de entrada de um nó no plano (Cja), através da Equação 4.4.

$$Cja = Ei \times Ce + P \times Cp \tag{4.4}$$

Sendo Pr a probabilidade de uma aresta conectada a um nó saindo da rede ser parte da rota até o pivô do nó no outro lado da aresta, então o custo médio de saída de um nó na rede (Cla) é dado pela Equação 4.5.

$$Cla = Ea \times Pr \times Ce + P \times Cp \tag{4.5}$$

Considerando que o custo de criação ne uma nova aresta bidirecional (Ce) é geralmente baixo, a saída ou entrada de nós no plano, em termos de número de mensagens trocadas ($Cjla$) pode ser aproximado pela Equação 4.6.

$$Cjla = \frac{4 \times E + 2}{N} - 2 \tag{4.6}$$

Como o total de arestas (E) é função do número médio de arestas por nó (Ea), o número de nós no plano (N), E pode ser calculado usando a Equação 4.7.

$$E = \frac{Ea \times N}{2} \tag{4.7}$$

Sendo assim, $Clja$ pode ser simplificado para a Equação 4.8.

$$Cjla = \frac{2}{N} + 2 \times Ea - 2 \tag{4.8}$$

Pode-se notar que conforme o crescimento de N, $Cjla$ tende a ser influenciado somente pelo número médio de arestas por nó (Ea), que independe do tamanho da rede. Este resultado indica que esta solução é escalável. Ainda, Ea também tende a ser um valor baixo, pois ele depende principalmente do número de arestas criadas por um nó que está entrando na rede (Ei). Obviamente este parâmetro pode ter seu valor atribuído a valores tão baixos como 2, e geralmente não há razões para que ele seja um valor mais alto.

Mesmo considerando o número de planos existentes ($Cjla$ deve ser multiplicado pelo número de planos existentes na rede), este valor ainda não invalida os resultados, pois o número de planos é controlado pelo número de grupos e pelo número de *score managers* existentes.

É importante ressaltar também que mesmo considerando o custo de criação de uma nova aresta no grafo (Ce) maior do que zero, o resultado final ainda é independente do número de nós (N), o que corrobora com a conclusão anterior.

4.6.2 Taxas de Pesquisa de Nós and Tamanho de Sessões

Em relação à pesquisa de *score managers*, o uso de redes magnéticas virtuais é claramente vantajoso em relação DHTs tradicionais, já que não há necessidade de comunicação, enquanto DHTs requerem $O(logN)$ na melhor das hipóteses (CHORD). As informações sobre os *score managers* já são conhecidas por cada nó, devido à natureza pró-ativa do algoritmo de propagação de força magnética.

No caso de redes magnéticas virtuais, todos os custos são transferidos para o mo-

mento de entrada ou saída da rede. Embora DHTs possam ter um custo constante nestas situações, observe que em $(1 - 2/N) \times 100$ por cento dos casos a rede magnética virtual exigirá apenas algumas operações de reconexão. Somente quando o nó que está entrando ou saindo da rede é o pivô (primário ou secundário), a propagação completa será necessária, e o custo de troca de mensagens será maior. Se considerarmos o uso da CAN para implementar a DHT (que é a implementação sugerida pela especificação original do EigenTrust (KAMVAR; SCHLOSSER; GARCIA-MOLINA, 2003)), o processo de saída de nós pode ser ainda mais caro, uma vez que é possível que nenhum dos vizinhos da área desocupada possa ocupar o espaço vazio, forçando uma "situação de *take-over*", em que não há limites superiores de tempo ou troca de mensagens para ser finalizada.

Como os tamanhos típicos de sessão (sessão é definido como sendo o ciclo entrar-participar-sair) em P2P redes estruturadas pode ser medido em horas, como mostrado em (STUTZBACH; REJAIE, 2006), e já que a probabilidade de que um pivô entre ou saia da rede é pequeno $(2/N)$, pode-se seguramente afirmar que as pesquisas por *score managers* superam de longe a necessidade de propagação devido a mudanças de pivô. Este fato torna a utilização de Redes Magnéticas Virtuais mais vantajosa do que DHTs neste contexto.

4.7 Conclusão

Foi apresentada uma alternativa aos DHTs para a seleção e a pesquisa de *score managers* no EigenTrust com base em Redes Magnéticas Virtuais. A solução proposta oferece uma alternativa proativa para este problema sem, no entanto, adicionar custos significativos para a entrada e saída de nós da rede, em particular considerando as características típicas do contexto analisado. Especificamente, o método remove a necessidade de pesquisa de nó para identificar os *score managers* de um nó específico. Como mostrado na Seção 4.6, o uso de campos magnéticos virtuais neste contexto traz um ganho real no desempenho médio da rede.

Capítulo 5

Avaliação e Aplicação de Reputação em Redes Magnéticas Virtuais

Tendo um sistema de confiança e reputação distribuído em cena, o próximo passo é determinar como será realizada a avaliação dos nós. Como esta avaliação é muito dependente da aplicação, o foco para esta questão está nas metodologias de como coletar estas avaliações, e não em como a avaliação é realizada.

Um fator importante de sistemas de confiança e reputação é que somente nós que prestam algum serviço podem ser avaliados. Tendo isto em vista, somente o nó pivô corrente é avaliado.

De modo geral, há três métodos para avaliação de serviços prestados por nós da rede. O primeiro é fazer com que o próprio cliente da solicitação avalie o serviço prestado pela rede e informe esta avaliação para o nó que recebeu inicialmente a solicitação, caso seja externo. O nó que recebeu a avaliação do cliente então consideraria esta avaliação como sua e a adicionaria à sua tabela de reputações.

Outra maneira de agregar avaliações é, caso a mensagem volte pelo mesmo caminho que chegou ao pivô, a avaliação por todos nós que encaminharam a mensagem de volta ou, caso não haja resposta em um tempo hábil para a aplicação em questão, uma avaliação negativa.

Um terceiro método, um pouco mais elaborado, seria factível somente em aplicações nas quais a força de atração deva ser reduzida significativamente e por tempo suficiente quando uma carga de trabalho é recebida. Caso isto ocorra, os outros nós da rede podem monitorar o nó que recebeu uma carga de trabalho e verificar se ele realmente propagou uma mensagem de redução de força na rede, como deveria. Em caso negativo, receberia uma avaliação negativa. Caso contrário, seria avaliado positivamente.

Tendo valores de reputação conhecidos globalmente para cada nó, o próximo passo é determinar como estes valores irão afetar a rede magnética virtual de modo que menos

mensagens sejam encaminhadas para os nós com baixa reputação, por mais que sua força de atração informada seja elevada. Para isso, nas próximas seções, são apresentados dois modelos básicos, o processo de pesquisa envolvido, os modelos de simulação utilizados, análise dos resultados da simulações e as conclusões relacionadas.

5.1 Modelo Transitivo

O primeiro modelo apresentado, chamado "transitivo", não apenas tenta evitar com que uma mensagem seja tratada por um nó com baixa reputação, mas também oferece resistência a que uma mensagem passe por ele até chegar ao pivô. Para que isso seja feito, sempre que um nó receber uma mensagem propagando a força de atração de outro nó, antes mesmo de qualquer outro tratamento, a força recebida será ponderada de acordo com a reputação do vizinho que o enviou a mensagem. Isto significa que quando o próximo nó receber uma nova mensagem de propagação de força, ele irá novamente ponderar o valor recebido, reduzindo-o ainda mais caso a reputação do nó que enviou a mensagem não seja 100%. Vale ressaltar que um nó sempre confiará 100% em si mesmo, logo sua própria força será considerada e propagada integralmente.

Na Figura 5.1, podemos ver um exemplo simplificado do modelo transitivo. O nó 1 inicia a propagação de sua nova força de atração (100) para o nó 2. O nó 2, ao receber a mensagem, pondera esta força de 100, usando a reputação do nó 1 (60%), considerando então sua força como 60. Como a força considerada do nó 3 é 56 (70% de 80) e sua própria força de atração é 50, o nó 1 será o novo pivô para o nó 2. No segundo momento, quando o nó 2 propaga esta informação para o nó 3, ele propagará que seu pivô é o nó 1, com força 60. O nó 3, ao receber esta mensagem, vai ponderá-la novamente, considerando a força do nó 1 como 54 (90% de 60), e vai continuar como sendo seu próprio pivô, pois possui força de 80.

No exemplo citado, percebe-se que, para os nós 1 e 2, o pivô será o nó 1, enquanto para o nó 3 o pivô será o próprio. Isto ocorre pois neste modelo, a tendência é que quanto mais longe estiver um nó de outro, menor será a força percebida entre eles. Isto faz com que exista a possibilidade de existir mais de um pivô, sendo que cada região da rede irá ter seu pivô. Isto pode ser um comportamento desejado, visto que neste caso existe menos chance de uma mensagem ser roteada por um caminho com baixa reputação, evitando possíveis descartes de mensagens neste caminho.

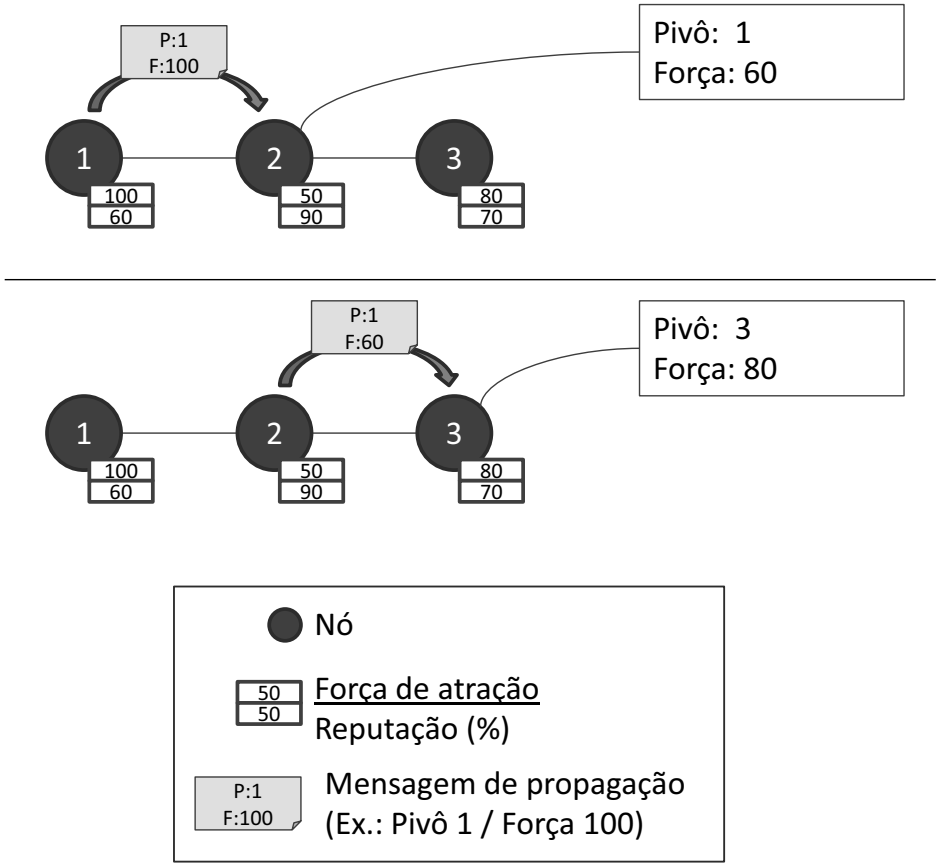


Figura 5.1: Exemplo do Modelo Transitivo.

5.2 Modelo Não-Transitivo

O segundo modelo, chamado "não-transitivo"trabalha de uma maneira diferente do primeiro: nenhuma força de atração é alterada quando propagada. Neste modelo, a reputação é usada para decidir quem na tabela de roteamento será o pivô, ao ponderar a força recebida nas mensagens de propagação usando a reputação do destino final a que esta rota levará. No caso de um nó passar para frente uma propagação de alteração de força, ele irá encaminhar com o pivô que foi selecionado após a ponderação, mas com sua força de atração original.

Na Figura 5.2 podemos ver um exemplo simplificado deste modelo. Assim como no exemplo anterior, o nó 1 inicia a propagação de sua nova força de atração (100) para o nó 2. O nó 2, ao receber a mensagem, pondera esta força de 100, usando a reputação do nó 1 (60%), considerando então sua força como 60 e o seleciona como seu pivô. O nó 2 então propaga este novo pivô para o nó 3, mas mantendo a força propagada como 100. O nó 3 então irá receber do nó 2 uma mensagem indicando que o nó 1 é o seu pivô e tem força 100. Neste momento, o nó 3 fará a ponderação da força recebida de acordo com a reputação do nó 1, resultando em uma força 60. Com uma força 60, o nó um será então

o novo pivô para o nó 3.

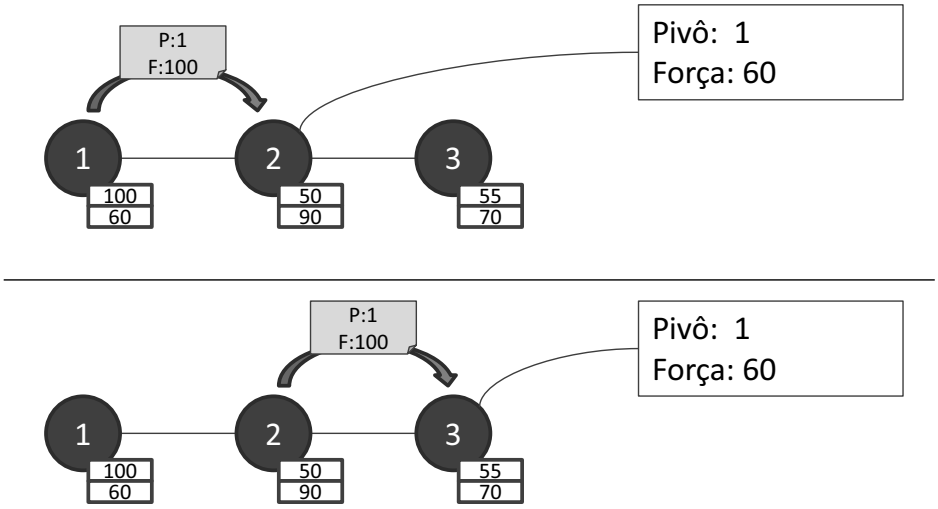


Figura 5.2: Exemplo do Modelo Não-Transitivo.

Diferentemente do modelo transitivo, neste modelo a tendência é que, após a estabilização da rede, todos os nós tenham como pivô ou um pivô global ou a si mesmo, caso a sua própria força não ponderada seja maior que a força ponderada do pivô global. Neste modelo não é levado em conta a reputação dos nós pelos quais as mensagens de carga de trabalho transitam.

5.3 Processo de Pesquisa e Desenvolvimento

Ambos os modelos, transitivo e não-transitivo, foram implementados usando como base o simulador de Redes Magnéticas Virtuais criado para simular o algoritmo Quick-Path (LIMA JR.; CALSAVARA, 2010), criado pelos autores deste algoritmo. As alterações descritas na sequência foram realizadas de forma a não afetar o funcionamento básico do algoritmo fazendo com que, caso todas as reputações forem configuradas para 100%, ele se comporte de forma idêntica ao simulador original.

O primeiro passo foi modificar o simulador para que cada nó possua um novo atributo que represente esta reputação, e que este atributo seja visível globalmente. Além disto, foi criado o suporte a um novo comando para os arquivos de simulação, com o objetivo de alterar o valor de reputação de um determinado nó. Desta maneira, o simulador representa a rede magnética virtual, assumindo que existe um sistema de confiança e reputação que fornece uma reputação global para cada nó, como o EigenTrust.

Tendo como base então este simulador alterado, durante o processo de desenvolvimento e testes foram encontradas algumas complicações ou problemas comuns aos modelos

transitivo e não-transitivo. O primeiro deles, foi encontrado nos primeiros testes em que se percebia que muitas das mensagens enviadas ao plano eram descartadas pela rede, pois as tabelas de rota geravam laços infinitos de roteamento de mensagens na rede. Após análise mais profunda, constatou-se que este cenário ocorre quando há mais de um nó com a força de atração máxima na rede, e diferentes nós no caminho que a mensagem deve percorrer possuem pivôs distintos. Para solucionar tal situação, alterou-se o simulador para que as mensagens de carga de trabalho sejam encaminhadas contendo um campo de "pivô preferido", que é atribuído pelo primeiro nó que recebe a mensagem. Neste campo é indicado o pivô escolhido inicialmente para este nó. Ao receber uma mensagem de carga de trabalho, os próximos nós verificam se este "pivô preferido"é também um dos possíveis pivôs de sua tabela, caso positivo, o encaminha para o caminho que a fará chegar neste pivô, caso contrário, altera este campo e encaminha para seu pivô preferido. Desta maneira as mensagens não são mais descartadas por roteamentos infinitos.

Uma segunda complicação encontrada comum aos dois modelos foi que após uma série de testes de carga com reputação perfeita, ao enviar 1000 mensagens para nós aleatórios em um plano com 100 nós conectados por *Small World* (WATTS; STROGATZ, 1998), por mais que a média de mensagens por nó fosse próxima de 10, o desvio padrão era alto, quando deveria ser zero ou muito próximo disso. Averiguou-se que a causa de tal comportamento era porque o algoritmo implementado para *Small World* neste simulador não gera um grafo fortemente conexo, como é pré-requisito para que esta condição seja satisfeita. Para isso foi alterado o algoritmo de geração de grafos para que ele gere todas as suas arestas como bidirecionais. Além disso, após a geração do grafo, é invocado um comando disponível no simulador que é usado para verificar a conectividade do grafo e, caso seja negativa, criar uma conexão entre as partes desconectadas. Esta parte do simulador também foi alterada para que gere arestas bidirecionais. Desta maneira, pode-se observar um bom resultado de simulação em caso de todas as reputações 100%.

Outra complicação ocorreu pelo tempo extremamente alto para que cada simulação terminasse. Após análise mais detalhada, foi constatado que a causa para tal comportamento era o excesso de conexões geradas pelo *Small World*. Os parâmetros enviados para a geração dos grafos estavam gerando um gráfico muito próximo de completo, o que reduz muito a vantagem de otimização de roteamento em Redes Magnéticas Virtuais. Após o ajuste da parametrização da geração dos grafos em *Small World*, os tempos voltaram a ser razoáveis.

Após os inícios dos testes de carga, agora aplicando a reputação ao grafo, independente do modelo, ocorriam muitos casos de mensagens sendo descartadas devido a roteamentos infinitos na rede. Após análise, constatou-se que a causa era que em um

certo ponto, após receber poucas mensagens, todos os nós tendiam a ter força de atração zero. Isso ocorre pois, nas simulações, cada mensagem é enviada para consumir 20% dos recursos disponíveis. Como a força de atração era um valor inteiro, significa que após 17 mensagens, um nó terá sua força de atração zerada. Junta-se a isso a aplicação da reputação, e os nós terão sua forças zeradas muito antes. Para tratar deste problema, a força foi substituída por uma variável de ponto flutuante. Desta maneira, por mais que as forças de atração seja baixas, elas ainda vão ser diferentes após um número grande de mensagens.

Para a simulação usando o modelo transitivo, foi alterada a maneira como as mensagens de propagação de força são tratadas. Ao receber uma mensagem deste tipo, antes de qualquer tratamento, agora são aplicadas as reputações. Desta maneira, com um mínimo de interferência no simulador, foi possível aplicar o modelo.

Para alterar o simulador para o modelo não-transitivo, a principal mudança foi realizada para que a escolha dos pivôs locais (principal e alternativo) seja embasada na força de atração ponderada pela reputação do pivô, alterando desta maneira o destino das mensagens de carga de trabalho, além do conteúdo das propagações de força, já que agora o nó pivô propagado pelo nó pode não ser mais o que tem maior força de atração em sua tabela.

Vale ressaltar que para ambos os modelos, sempre os nós irão considerar a sua própria reputação como 100%, independente do valor informado pelo sistema de confiança e reputação.

Para a geração de dados de teste e processamento dos resultados, foram utilizadas planilhas eletrônicas. Elas são utilizadas para a geração de curvas de reputação, geração de mensagens e configuração dos arquivos de simulação. Em suas primeiras versões, esta planilha era capaz de gerar somente um arquivo de simulação por vez, sendo que a criação dos arquivos de simulação era feita de maneira manual, utilizando a funcionalidade de copiar e colar do conteúdo destas planilhas. Nas versões posteriores, utilizando ferramentas de programação, ela foi adaptada para gerar os arquivos diretamente e, de forma automática, gerar todos os arquivos necessários (1000 arquivos por geração) para a repetição da execução dos testes nas simulações.

Estas planilhas também são responsáveis pelo processamento e apresentação dos resultados. Nas versões iniciais, a planilha era capaz de, tendo a lista de nós que trataram cada mensagem colada em uma de suas colunas, processar esta informação e plotar gráficos de acordo. Nas versões posteriores, a importação de dados era feita diretamente dos arquivos de saída da simulação e realizando a consolidação destes dados em uma de suas colunas. Este procedimento, realizado através de programação dentro da ferramenta,

também é capaz de listar e gerar estatísticas de quantidade de mensagens descartadas em cada simulação, permitindo detectar as complicações citadas quando ocorreram. Após a consolidação dos dados pela planilha, os gráficos de resultados eram automaticamente gerados.

Para a execução dos arquivos de simulação no simulador e coleta dos resultados, foi criado um *shell script*, capaz de, em suas primeiras versões, executar sequencialmente todos os arquivos de simulação disponíveis, filtrar os resultados e gravá-los em formato de arquivo compatível com as planilhas citadas. Em uma versão posterior, foi implementado neste *shell script* a capacidade de execução paralela das simulações, para reduzir o tempo total das execuções de cada bloco de simulações.

Após a execução das simulações com as correções e ajustes citados, notou-se comportamentos dos resultados das simulações que, além de muito similares entre os dois modelos, apresentam curvas de resultado ligeiramente diferentes do esperado. Para tentar isolar a causa, inicialmente utilizou-se uma curva de reputações com crescimento linear de 0% a 100%. Com esta curva, pode-se observar a tendência "natural"que os modelos geravam.

Com a tendência natural diferente do esperado, buscou-se então isolar uma segunda possível causa deste comportamento: o "narcisismo"dos nós, ou seja, o fato de sempre se considerarem 100% confiáveis. Para isto, modelou-se o sistema como se ele fosse somente um mecanismo de descoberta, e não de roteamento de mensagens. Isto significa que caso o nó que recebe a mensagem inicialmente não a trate, ela é encaminhada diretamente ao pivô conhecido por este nó, diminuindo o número de mensagens que são tratadas antes de chegar ao pivô esperado. Embora esta alteração tenha melhorado o comportamento nos dois modelos, a tendência "natural"das curvas continuavam iguais.

A suspeita seguinte para este comportamento foi o modelo de consumo de força de atração dos nós ao receber uma carga de trabalho. Para isolar este fator, novas simulações foram realizadas. Nelas o consumo da força de atração se dava de maneira linear, ou seja, a cada mensagem um número constante era consumido, tomando o cuidado para que este número fosse baixo o suficiente para que com a média de mensagens recebidas por cada nó, a força termine a simulação com valor significativamente acima de zero, sendo a única exceção para o caso em que um nó receba todas as mensagens encaminhadas para a rede. Neste caso as simulações, apesar de mais próximas do ideal, ainda possuíam uma tendência distorcida do esperado, principalmente para o caso com reputações com crescimento linear.

Para identificar a diferença de comportamento entre os dois modelos, foram realizadas novas simulações, mas desta vez tendo todos os nós com mesma reputação, sendo

três simulações feitas para cada modelo, com 25%, 50% e 75% de reputação. Nestas novas simulações, para cada execução foi realizada a ordenação da contagem de mensagens de cada nó, para que sejam consolidadas ordenadas por *ranking*. Ou seja, para cada execução, o primeiro valor será a contagem de mensagens tratadas pelo nó que mais tratou mensagens, a segunda pelo nó que tratou o segundo maior número de mensagens, e sucessivamente. Com estes dados é possível analisar a distribuição de mensagens no grafo.

Percebeu-se que a diferenciação dos dois modelos ocorre principalmente quando a reputação média da rede é mais alta. Por isso, para se obter um resultado mais granular nesta faixa, repetiu-se o experimento, mas agora com reputações constantes em 85% e 100%. Tendo estes dados, realizou-se então a consolidação em novos gráficos.

5.4 Modelo de Simulação

Para validar os modelos propostos, foram realizadas diversas simulações usando diferentes distribuições de reputação e diferentes modelos de distribuição de mensagens de carga de trabalho na rede.

A topologia da rede nas simulações foi gerada aleatoriamente em cada uma das execuções, utilizando o algoritmo *Small World* (WATTS; STROGATZ, 1998) para geração dos grafos. Na montagem da topologia, todas as arestas criadas foram bidirecionais, e ainda, após a topologia montada, foi executada uma verificação automática de conectividade do grafo. Caso esta verificação falhasse, seria então criada uma nova conexão bidirecional aleatória ligando as áreas desconectadas da rede. Como parâmetros para o *Small World*, cada nó se conectou inicialmente com os 3 nós mais próximos, com chance de 2% de realizar uma conexão aleatória. O *Small World* foi utilizado para a criação da topologia pois permite a aleatoriedade do grafo ao mesmo tempo que mantém uma rede com baixo número de saltos ligando os nós, de maneira simples e eficiente.

Cada simulação consistiu de grafo de vizinhanças com 100 nós, todos eles inicialmente com uma força de atração 100 (com o valor da força permitindo valores decimais), e com reputações definidas pelas curvas apresentadas na sequência, partindo do nó com o identificador mais baixo (nó 1) possuindo a menor reputação, até o nó com o identificador mais alto (nó 100) com a maior reputação do plano. Em cada simulação 1000 mensagens foram enviadas em sequência ao plano. Nas simulações iniciais, cada mensagem, ao ser tratada, reduz 20% da força de atração restante do nó. Nelas foram escolhidos três cenários para escolher o destino das mensagens: no primeiro, cada mensagem possuía como destino um nó aleatório entre os 100 possíveis. No segundo modelo, todas as men-

sagens são encaminhadas para o nó com menor reputação na rede (nó 1), e no terceiro modelo todas as mensagens são encaminhadas para o nó com maior reputação na rede (nó 100). Para estas simulações, foram utilizadas cinco curvas diferentes de reputações atribuídas aos nós, apresentadas a seguir.

A primeira curva de reputação, observada na Figura 5.3, tem os primeiros nós com reputação abaixo de 40%, mas com uma elevação rápida, chegando a 100% já no quadragésimo terceiro nó. Este modelo representa uma rede com reputação média de 95,5%, simulando um modelo com poucos nós com comportamento danoso.

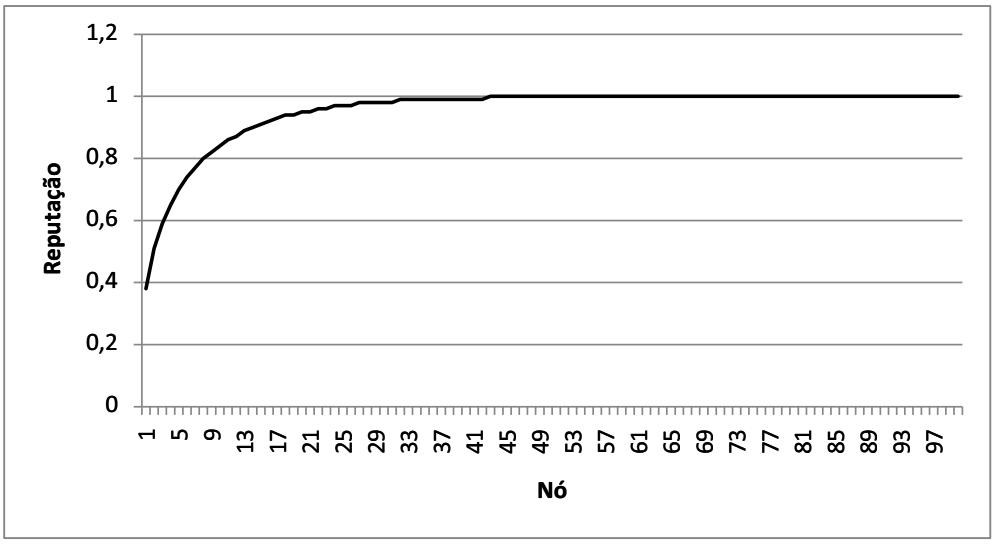


Figura 5.3: Curva de reputação onde a média das reputações é 95,5%.

A segunda curva de reputação, observada na Figura 5.4, tem um formato similar à primeira, mas com reputações com crescimento mais lento. O primeiro nó tem reputação de somente 22%, crescendo até o último com 98%. Este modelo representa uma rede com reputação média de 83,8%. Ele tem a grande maioria dos nós com comportamento bom ou excelente, e alguns com reputação muito baixa.

A terceira curva de reputação, observada na Figura 5.5, traz poucos nós com reputações mais altas, e a maioria com reputações médias e boas. Nesta curva, a reputação média é de 77,8%.

A quarta curva de reputação, representada pela Figura 5.6, traz um cenário com muito poucos nós com boa reputação e a maior parte dos nós com reputação abaixo de 60%. Com uma média de reputação de 48,4%, este cenário serve como base para avaliar o comportamento do sistema em uma situação de baixa reputação na rede.

Na quinta e última curva de reputação, representada pela Figura 5.7, mostra o caso de crescimento linear da reputação, partindo de 0% à 100%. Neste caso, a média

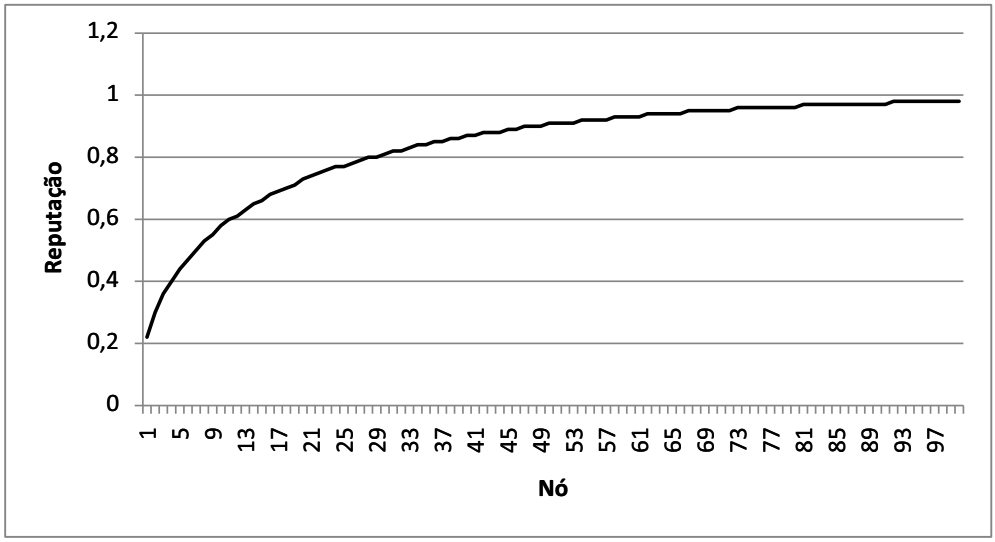


Figura 5.4: Curva de reputação onde a média das reputações é 83,8%.

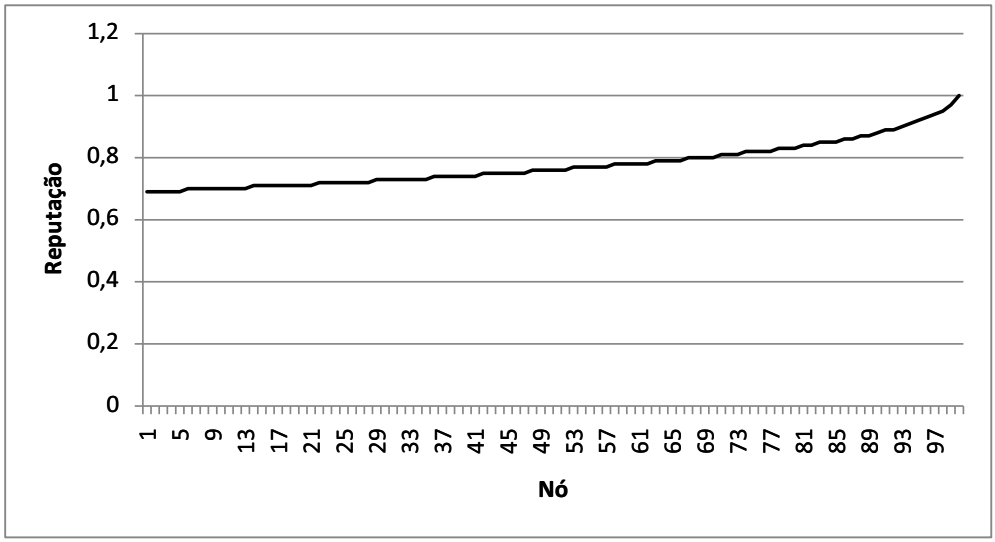


Figura 5.5: Curva de reputação onde a média das reputações é 77,8%.

de reputações é exatamente 50%. Este caso é utilizado para avaliar as distorções geradas pelos modelos de acordo com um resultado esperado linear.

Em um segundo conjunto de simulações, foi alterada a forma como as mensagens são encaminhadas na rede, de forma que as mensagens, ao chegar externamente a um nó, serão encaminhados por ele diretamente ao pivô de sua tabela. Utilizou-se este comportamento para simular a rede sendo usada somente para descoberta, e não para roteamento de mensagens com carga de trabalho. Neste bloco de simulações, foram utilizadas as mesmas curvas de reputação apresentadas anteriormente, mas foram realizadas somente as simulações no caso de entrega para o nó com o identificador mais alto (e portanto maior reputação). Isto se deve à conclusão de que o comportamento para entrega no nó com

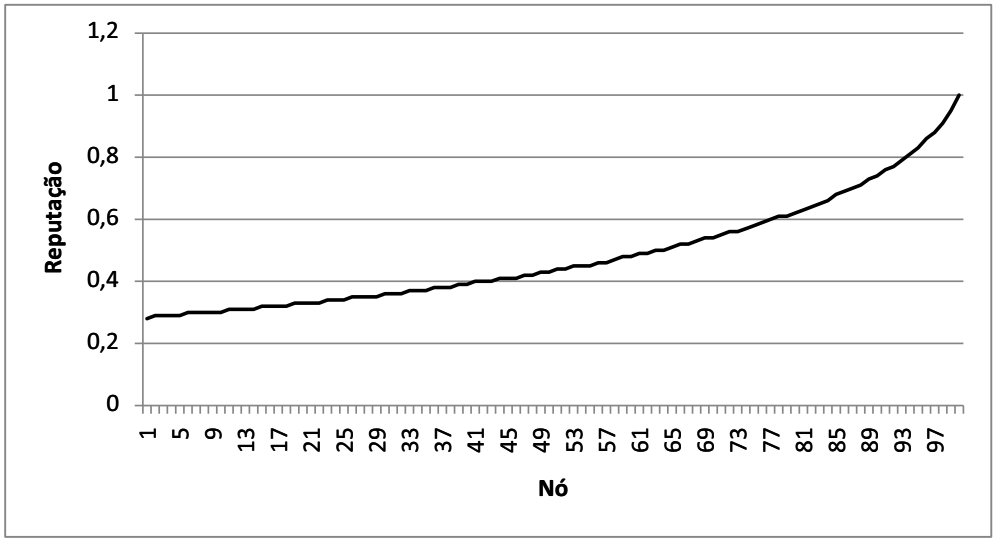


Figura 5.6: Curva de reputação onde a média das reputações é 48,4%.

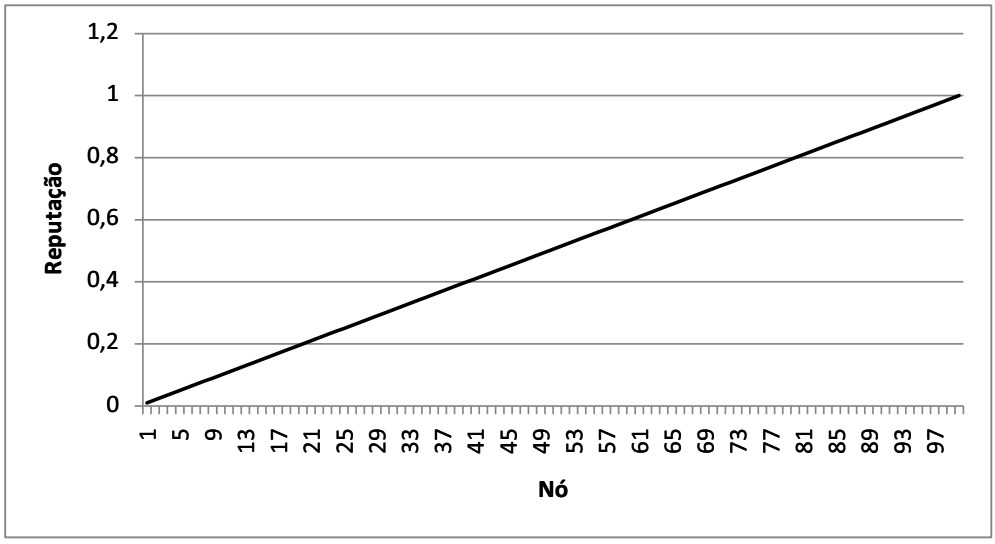


Figura 5.7: Curva de reputação com reputações com crescimento linear.

o menor identificador, tem resultados praticamente idênticos às simulações que entregam no nó com o maior identificador, exceto que o pico de mensagens muda de nó. O caso de entrega aleatória também não se faz necessário, pois evidencia o comportamento narcisista do nó em reter as mensagens que recebe, tornando os gráficos de resultado distorcidos.

Em um terceiro conjunto de simulações, partindo das simulações básicas, foi alterada a maneira que a força de atração é consumida pelas mensagens. Nelas, cada mensagem subtraia 5% da força de atração, possibilitando então que cada nó trate até 20 mensagens até chegar a 0 de força de atração. Nestas simulações foram utilizadas as mesmas curvas de reputação, mas nos casos de chegada de mensagens no nó com maior identificador e em um nós aleatórios.

No quarto conjunto de simulações, foram utilizadas curvas de reputação com valores iguais para todos os nós, sendo eles 20%, 50%, 75%, 85% e 100%, executados tendo como base as condições do primeiro bloco de simulações. Nestas simulações, além de analisados os gráficos de distribuição de mensagens por nó, foram criados novos gráficos de número de mensagens por *ranking* de mensagens recebidas, isto é, para cada uma das execuções do algoritmo, o vetor número de mensagens recebidas por nó é reordenado de acordo com o total de mensagens e consolidado em um vetor de *ranking*. Isto se traduz em gráficos que no eixo Y trazem o número de mensagens e no eixo X trazem o *ranking* de recebimento, sendo 1 o *ranking* que mais recebeu mensagens, 2 o que segundo mais recebeu e assim sucessivamente. Nestas simulações foram utilizados somente os casos de chegada de mensagens exclusivamente no nó de maior identificador, pelos motivos citados.

5.5 Resultados de Simulação

Os resultados obtidos do primeiro conjunto de simulações são mostrados nos gráficos das Figuras 5.8 a 5.17. Em cada figura, o gráfico (a) mostra a média dos resultados quando o ponto de entrada de mensagens na rede é o nó de maior reputação; o gráfico (b), quando o ponto de entrada é o nó de menor reputação; e o gráfico (c), quando cada uma das 1000 mensagens é distribuída de forma aleatória entre os 100 nós. Somente nos gráficos com curva de reputação com reputações com crescimento linear (Figura 5.7), os gráficos de quando o ponto de entrada é o nó de menor reputação são omitidos, sendo o gráfico (b) o resultado da simulação de quando cada uma das 1000 mensagens é distribuída de forma aleatória entre os 100 nós.

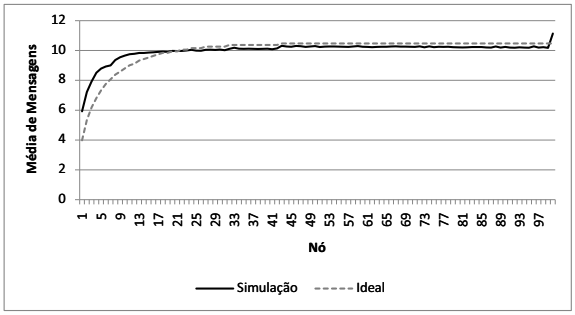
Em todos os gráficos apresentados nesta seção, a linha tracejada representa a distribuição ideal de mensagens para a respectiva configuração de reputações. Ela é calculada a partir da curva de reputação dos nós, considerando quanto é o seu peso em número de mensagens de um total de 1000 mensagens na simulação. A linha contínua representa a média simples das 1000 simulações de cada caso.

As Figuras 5.18 e 5.19 fazem parte do resultado do segundo conjunto de simulações, em que as mensagens são entregues diretamente ao pivô. Nestas figuras, temos todas as simulações com todas as mensagens chegando no nó de maior reputação. Nos gráficos, são exibidos, respectivamente, o resultado de simulação para as curvas de reputação onde a média das reputações é 95,5% (Figura 5.3), 83,8% (Figura 5.4), 77,8% (Figura 5.5) e 48,4% (Figura 5.6).

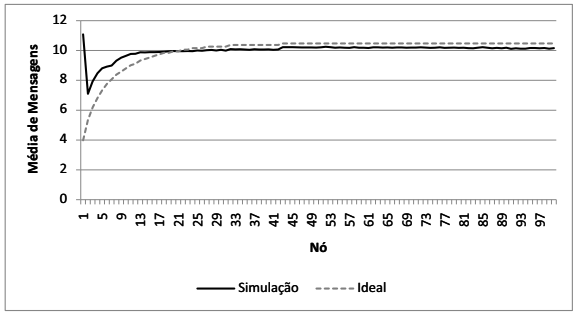
Os resultados obtidos do terceiro bloco de simulações, em que a força é subtraída dos nós linearmente, são mostrados nos gráficos das Figuras 5.20 a 5.25. Em cada figura,

o gráfico (a) mostra a média dos resultados quando o ponto de entrada de mensagens na rede é o nó de maior reputação; e o gráfico (b), quando cada uma das 1000 mensagens é distribuída de forma aleatória entre os 100 nós.

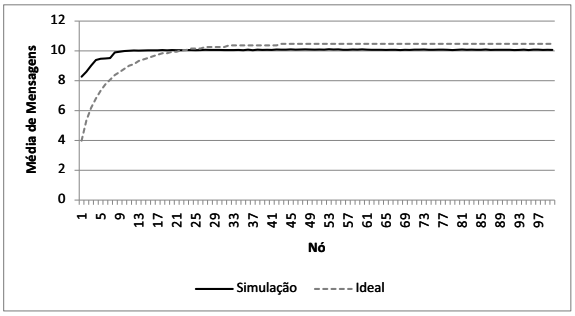
A Figura 5.26 mostra um gráfico comparativo entre as simulações com reputação constante em 75% e 85% nos modelos transitivo e não transitivo, ordenado por *ranking*, conforme descrito na Seção 5.4.



(a) Mensagens chegando no nó de maior reputação

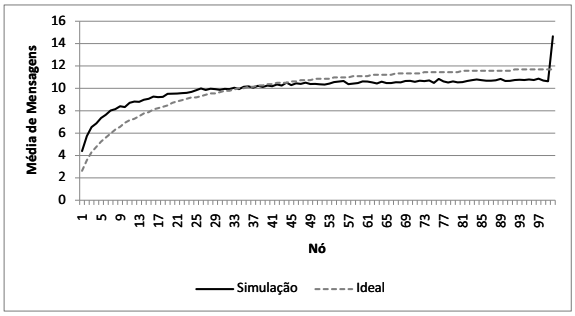


(b) Mensagens chegando no nó de menor reputação

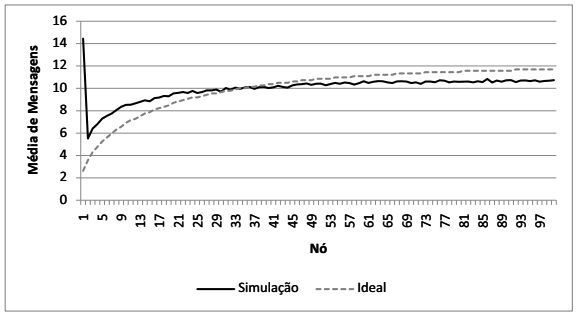


(c) Mensagens chegando em nós aleatórios

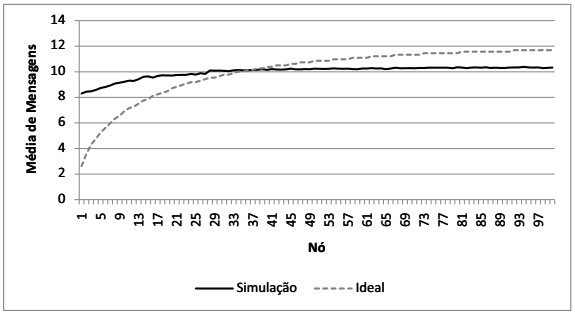
Figura 5.8: Distribuição de mensagens com curva de reputação onde a média das reputações é 95,5% (Figura 5.3) no modelo transitivo



(a) Mensagens chegando no nó de maior reputação

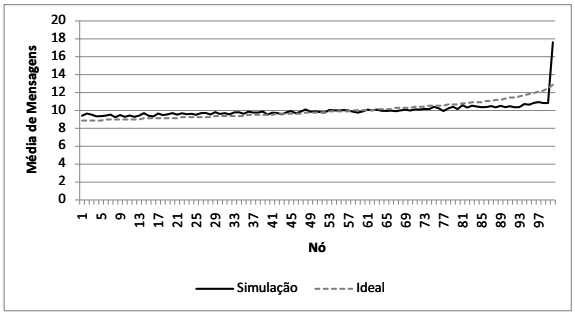


(b) Mensagens chegando no nó de menor reputação

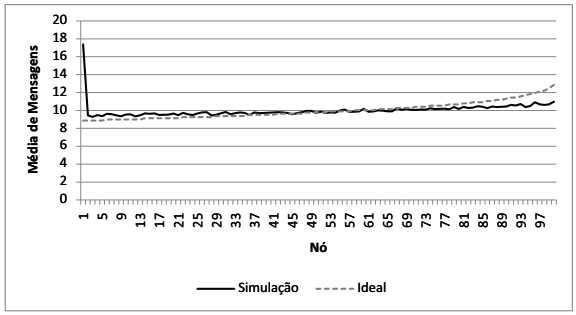


(c) Mensagens chegando em nós aleatórios

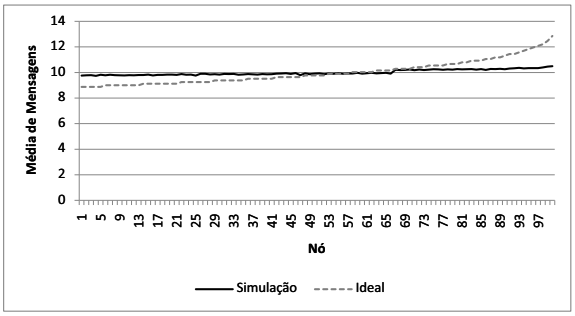
Figura 5.9: Distribuição de mensagens com curva de reputação onde a média das reputações é 83,8% (Figura 5.4) no modelo transitivo



(a) Mensagens chegando no nó de maior reputação

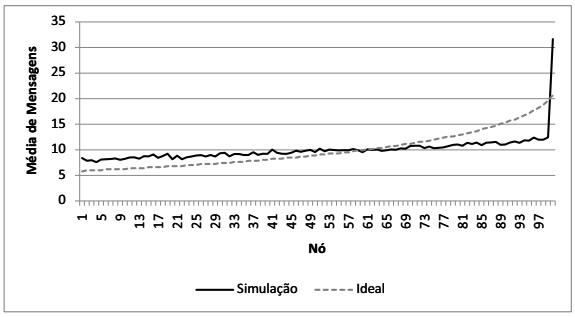


(b) Mensagens chegando no nó de menor reputação

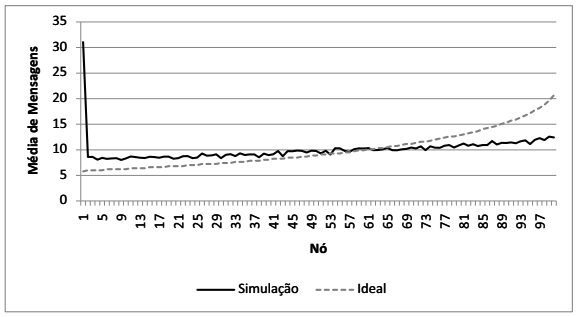


(c) Mensagens chegando em nós aleatórios

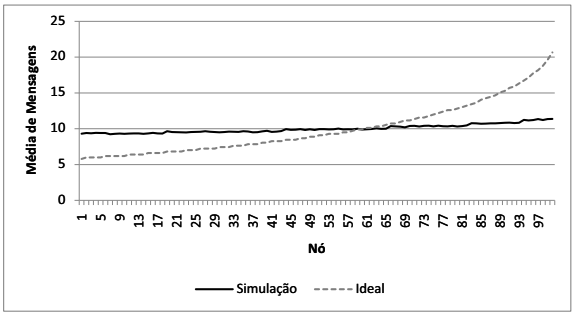
Figura 5.10: Distribuição de mensagens com curva de reputação onde a média das reputações é 77,8% (Figura 5.5) no modelo transitivo



(a) Mensagens chegando no nó de maior reputação

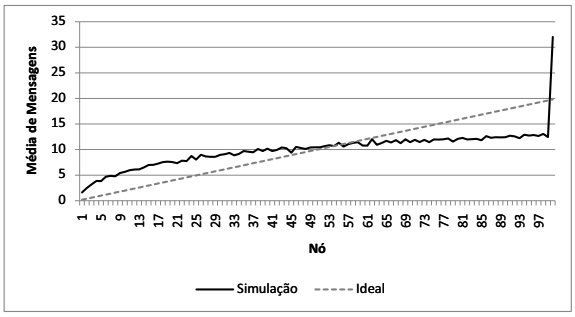


(b) Mensagens chegando no nó de menor reputação

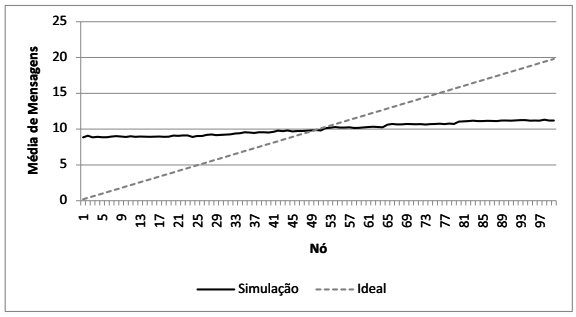


(c) Mensagens chegando em nós aleatórios

Figura 5.11: Distribuição de mensagens com curva de reputação onde a média das reputações é 48,4% (Figura 5.6) no modelo transitivo

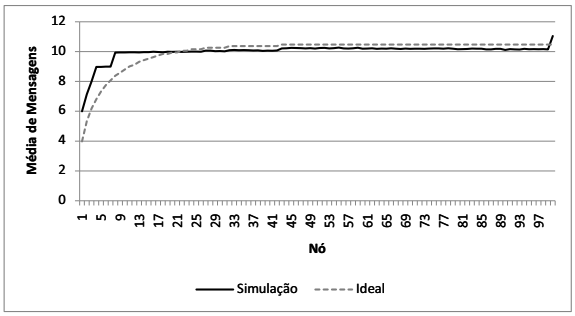


(a) Mensagens chegando no nó de maior reputação

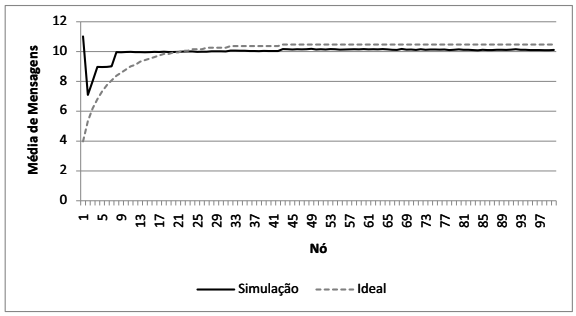


(b) Mensagens chegando em nós aleatórios

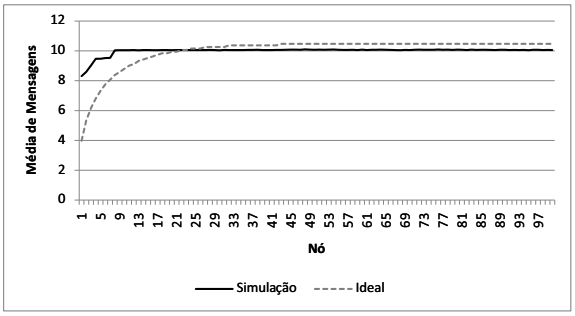
Figura 5.12: Distribuição de mensagens com curva de reputação com reputações com crescimento linear (Figura 5.7) no modelo transitivo



(a) Mensagens chegando no nó de maior reputação

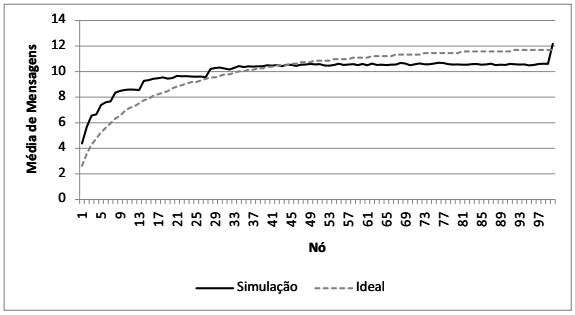


(b) Mensagens chegando no nó de menor reputação

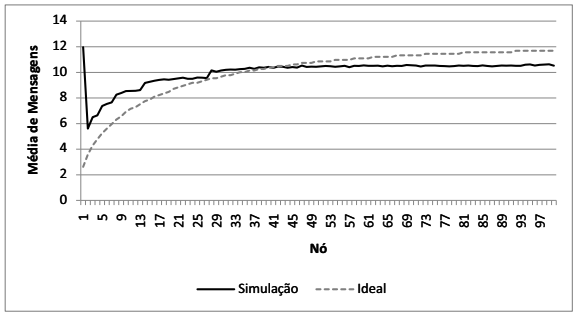


(c) Mensagens chegando em nós aleatórios

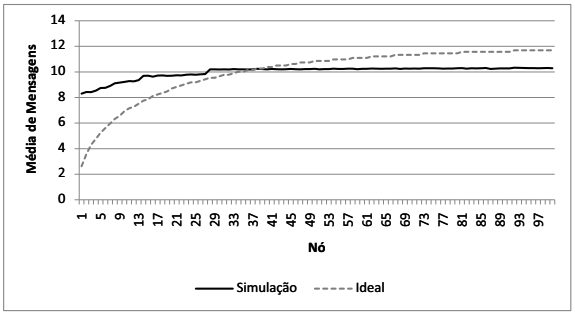
Figura 5.13: Distribuição de mensagens com curva de reputação onde a média das reputações é 95,5% (Figura 5.3) no modelo não-transitivo



(a) Mensagens chegando no nó de maior reputação

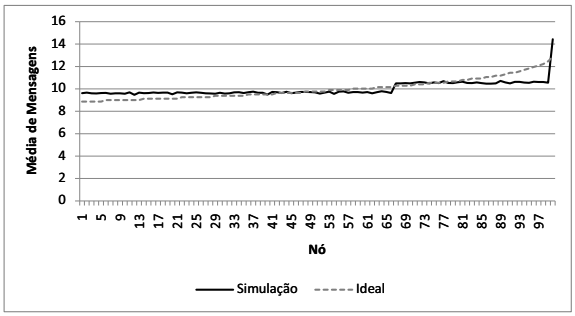


(b) Mensagens chegando no nó de menor reputação

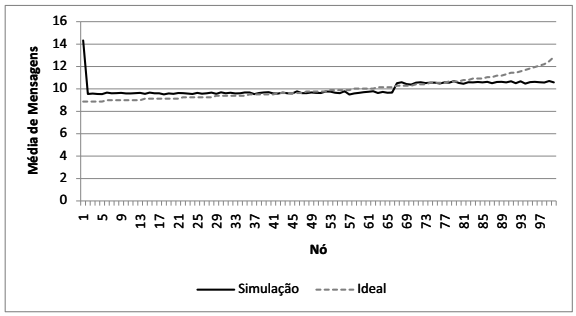


(c) Mensagens chegando em nós aleatórios

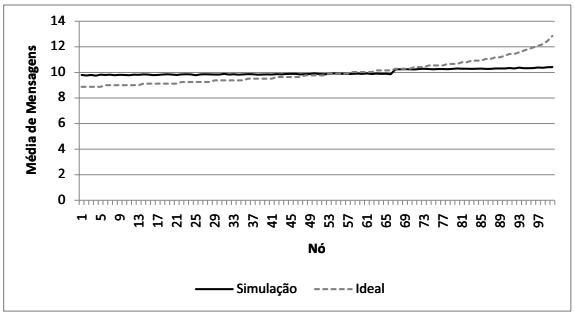
Figura 5.14: Distribuição de mensagens com curva de reputação onde a média das reputações é 83,8% (Figura 5.4) no modelo não-transitivo



(a) Mensagens chegando no nó de maior reputação

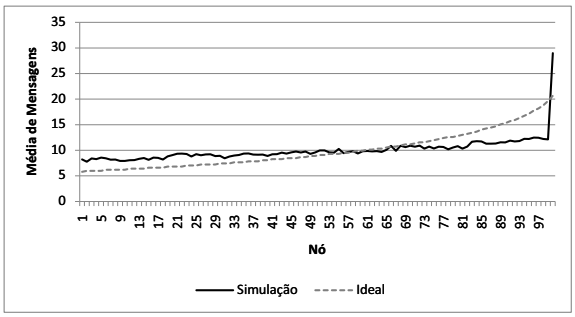


(b) Mensagens chegando no nó de menor reputação

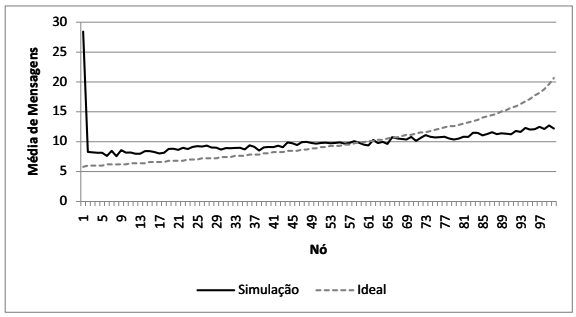


(c) Mensagens chegando em nós aleatórios

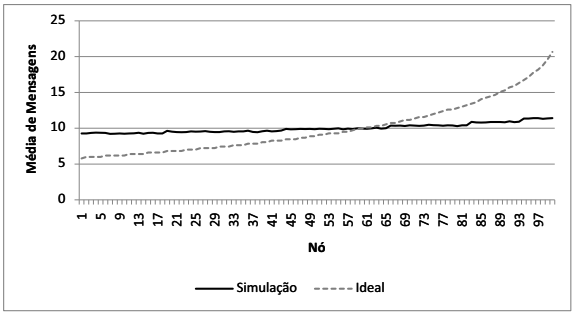
Figura 5.15: Distribuição de mensagens com curva de reputação onde a média das reputações é 77,8% (Figura 5.5) no modelo não-transitivo



(a) Mensagens chegando no nó de maior reputação

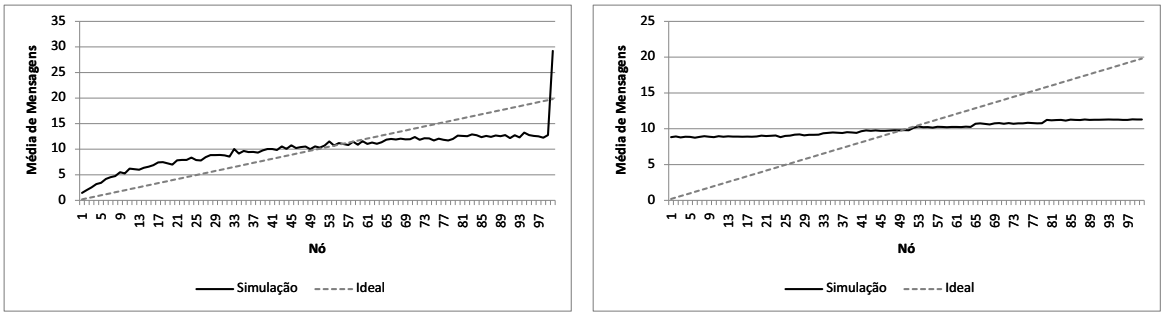


(b) Mensagens chegando no nó de menor reputação



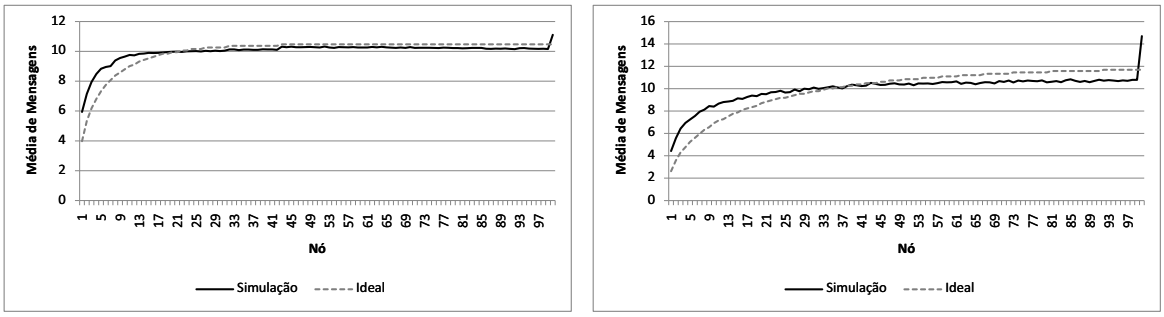
(c) Mensagens chegando em nós aleatórios

Figura 5.16: Distribuição de mensagens com curva de reputação onde a média das reputações é 48,4% (Figura 5.6) no modelo não-transitivo



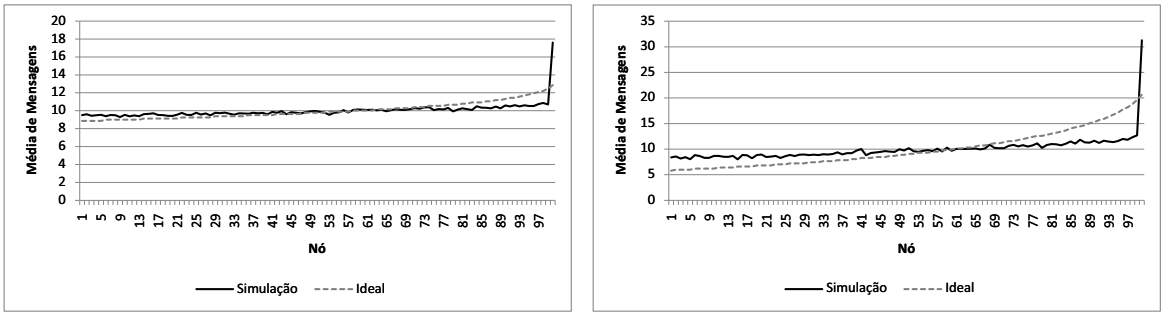
(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.17: Distribuição de mensagens com curva de reputação com reputações com crescimento linear (Figura 5.7) no modelo não-transitivo



(a) Curva de reputação onde a média das reputações é 95,5% (Figura 5.3)

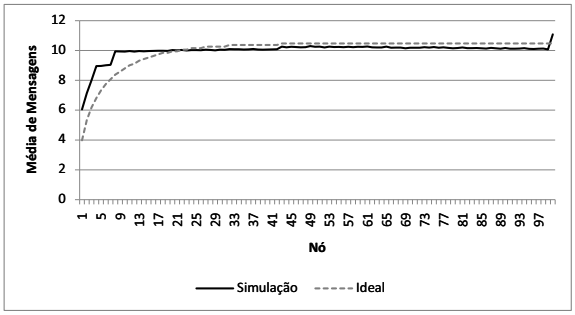
(b) Curva de reputação onde a média das reputações é 83,8% (Figura 5.4)



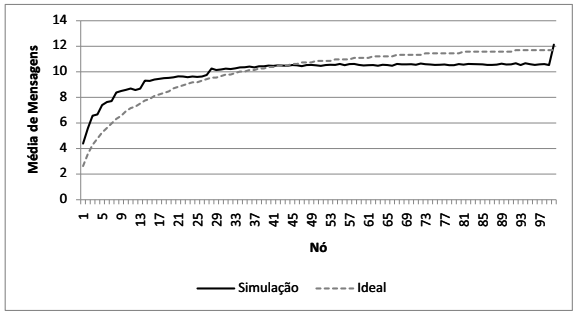
(c) Curva de reputação onde a média das reputações é 77,8% (Figura 5.5)

(d) Curva de reputação onde a média das reputações é 48,4% (Figura 5.6)

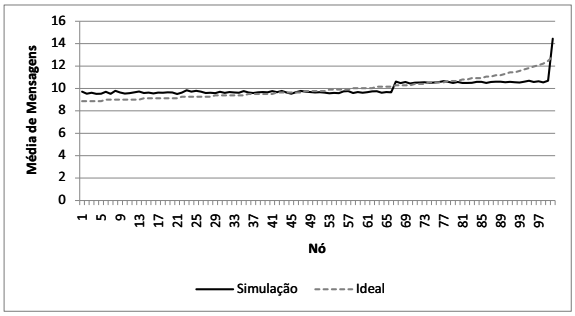
Figura 5.18: Distribuição de mensagens com entrega direta para o pivô no modelo transitivo



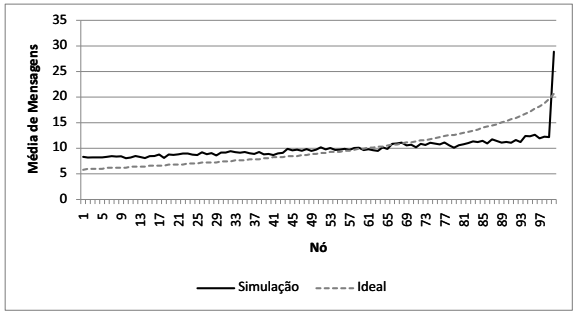
(a) Curva de reputação onde a média das reputações é 95,5% (Figura 5.3)



(b) Curva de reputação onde a média das reputações é 83,8% (Figura 5.4)

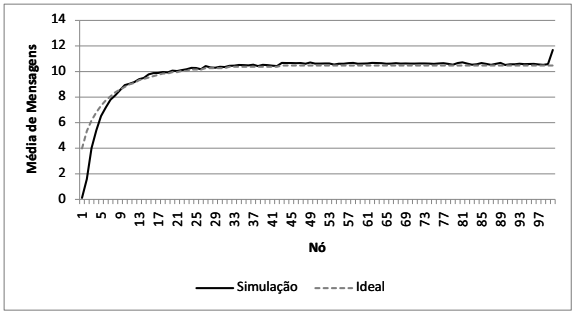


(c) Curva de reputação onde a média das reputações é 77,8% (Figura 5.5)

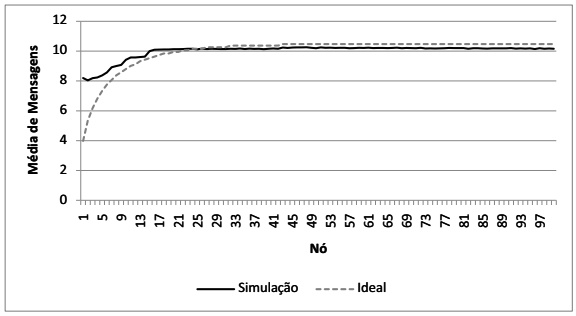


(d) Curva de reputação onde a média das reputações é 48,4% (Figura 5.6)

Figura 5.19: Distribuição de mensagens com entrega direta para o pivô no modelo não-transitivo

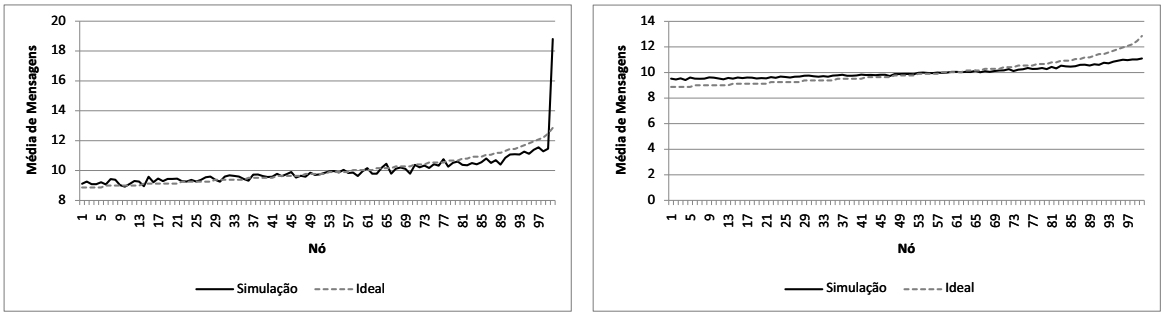


(a) Mensagens chegando no nó de maior reputação



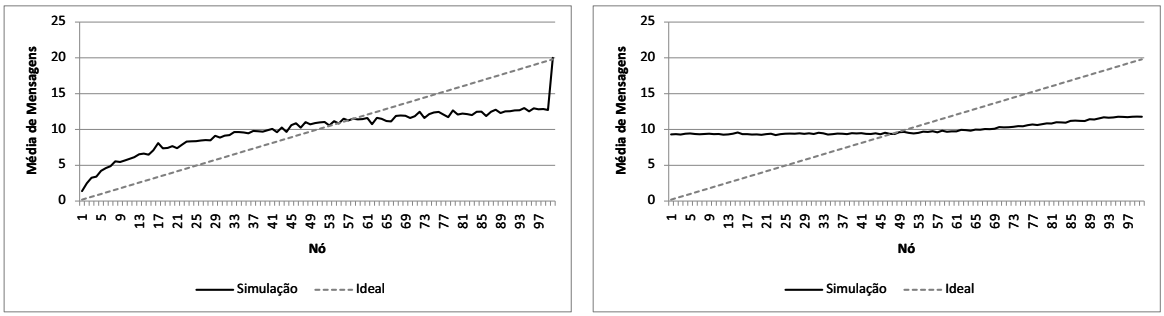
(b) Mensagens chegando em nós aleatórios

Figura 5.20: Distribuição de mensagens com curva de reputação onde a média das reputações é 95,5% (Figura 5.3) no modelo transitivo com consumo linear de força de atração



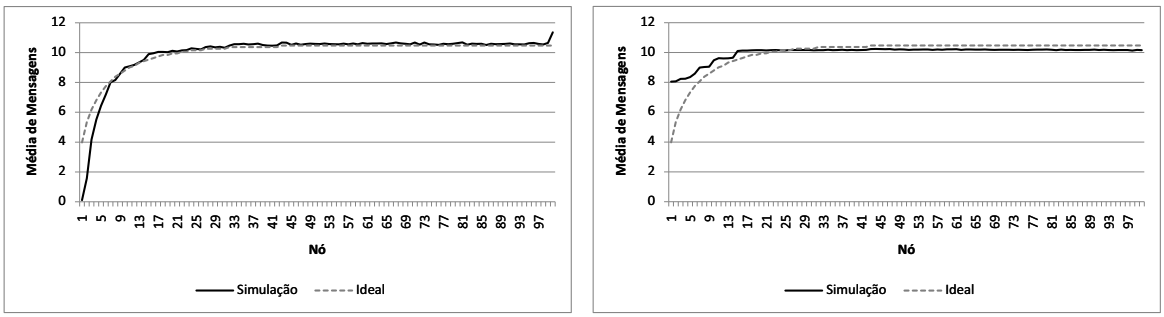
(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.21: Distribuição de mensagens com curva de reputação onde a média das reputações é 77,8% (Figura 5.5) no modelo transitivo com consumo linear de força de atração



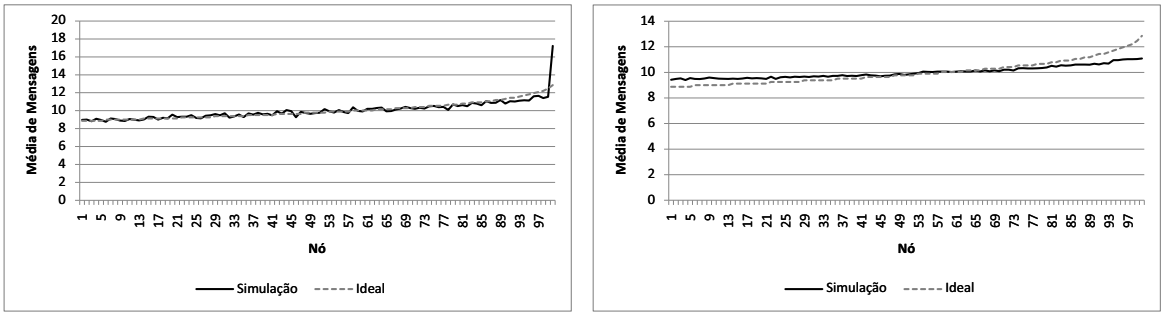
(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.22: Distribuição de mensagens com curva de reputação com reputações com crescimento linear (Figura 5.7) no modelo transitivo com consumo linear de força de atração



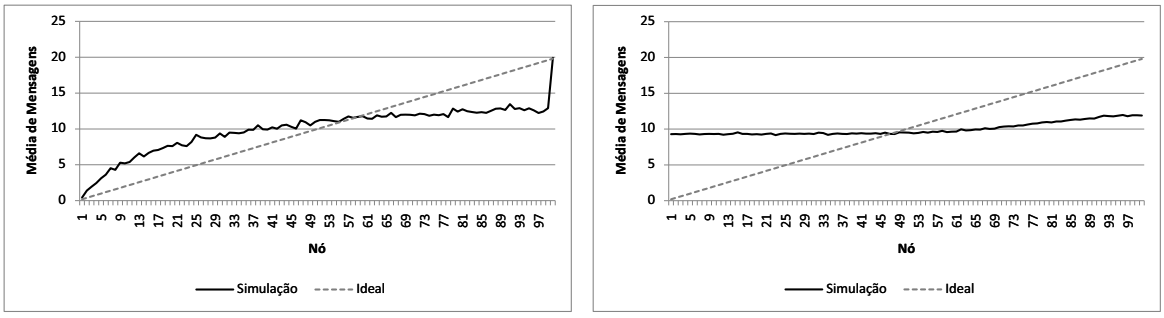
(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.23: Distribuição de mensagens com curva de reputação onde a média das reputações é 95,5% (Figura 5.3) no modelo não-transitivo com consumo linear de força de atração



(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.24: Distribuição de mensagens com curva de reputação onde a média das reputações é 77,8% (Figura 5.5) no modelo não-transitivo com consumo linear de força de atração



(a) Mensagens chegando no nó de maior reputação (b) Mensagens chegando em nós aleatórios

Figura 5.25: Distribuição de mensagens com curva de reputação com reputações com crescimento linear (Figura 5.7) no modelo não-transitivo com consumo linear de força de atração

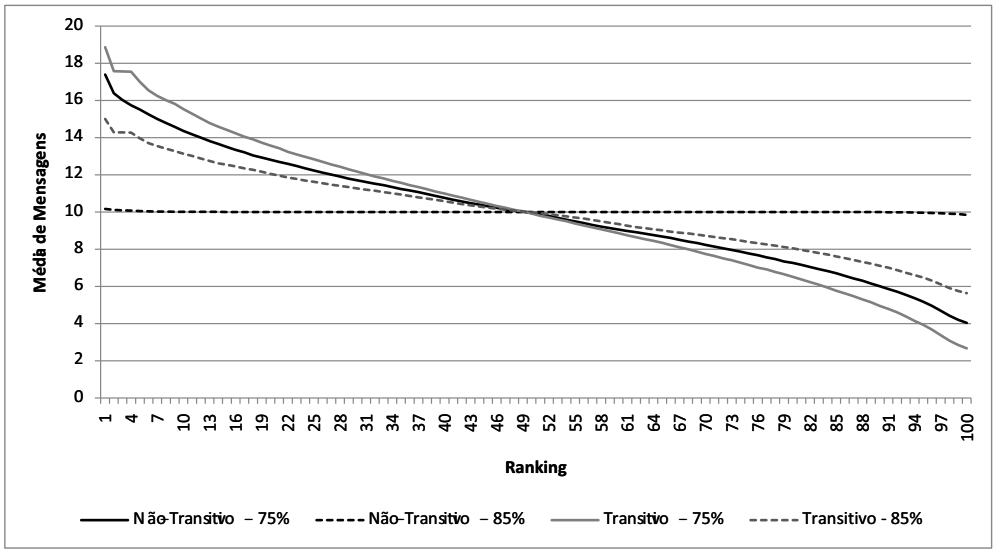


Figura 5.26: Comparação ordenada por *ranking* com reputação constante em 70% e 85%

5.6 Análise dos Resultados de Simulação

A partir dos gráficos apresentados, uma sequência de observações e conclusões podem ser traçadas. Ao observar os gráficos de distribuição de mensagens do modelo transitivo (Figuras 5.8 a 5.11), e compará-los com os do modelo não-transitivo (Figuras 5.13 a 5.16), nota-se que ambos possuem comportamento muito similar. Mesmo com simulações com entrega direta do nó que recebe a mensagem ao pivô (Figuras 5.18 e 5.19), ou então com simulações com um modelo de consumo de força de atração linear (Figuras 5.20 a 5.25), e também quando se utiliza reputação idêntica em todos os nós pode-se notar a grande similaridade (Figura 5.26). Após análise mais crítica deste conjunto de simulações, e eliminando os fatores citados, supõe-se que o fator principal causador deste comportamento seja a alta conectividade dos grafos utilizados, em que cada nó se conecta aos 3 nós vizinhos mais próximos, e ainda tem 2% de chance de se conectar a outro nó aleatório. Pelo número de saltos médio na rede ser baixo, o efeito transitivo não seria tão perceptível nas simulações. Em trabalhos futuros pretende-se analisar esta possibilidade.

Nota-se no entanto, nos casos em que há chegada de mensagens em um único nó, que o número de mensagens tratadas por este nó é maior no modelo transitivo do que no não-transitivo (comparar a Figura 5.10a com a Figura 5.15a). É perceptível que esta diferença se acentua conforme a reputação média da rede diminui. Estes picos no nó que recebe a mensagem são naturais, pois a força considerada para si mesmo é sempre não ponderada pela sua reputação. Tendo isto em vista, ele tende a reter mais mensagens do que os outros nós. Este comportamento é acentuado no modelo transitivo pois o nó que recebe as mensagens tende a confiar menos nos outros nós da rede. O mesmo motivo é a causa de haver picos maiores conforme a reputação média da rede é reduzida.

Em contrapartida, se observarmos os gráficos com distribuição aleatória de mensagens entre os nós, percebemos que as linhas ficam mais próximas de uma distribuição mais igualitária, independente da reputação (por exemplo, na Figura 5.10c). Este comportamento novamente é causado pelo narcisismo dos nós (i.e. considerar sua própria reputação perfeita). Neste caso, cada nó tem a tendência de tratar a mensagem que recebe, antes de repassá-la a um nó com a mesma força, por mais que este outro nó tenha reputação maior.

Outro efeito observado do narcisismo dos nós é que em gráficos com reputações médias mais baixas, o comportamento é mais distante da curva ideal, e mais próxima de uma curva igualitária (Figuras 5.11 e 5.16).

Nos gráficos de distribuição de mensagens por nó pode-se observar, principalmente no modelo não-transitivo, que se formam "degraus"conforme o crescimento da reputação

dos nós (Figura 5.13). Isto acontece pois, apesar dos gráficos representarem a média de mensagens, o número de mensagens recebida por nó ainda é um número inteiro. Levando isto em conta, caso haja um distribuição similar entre a grande maioria das simulações, não é possível que uma curva acompanhe a curva ideal. Os "degraus"mostram que, no caso não-transitivo, existe uma distribuição mais uniforme entre as execuções.

Ao observar os gráficos que apresentam curvas de reputação com reputações com crescimento linear (Figura 5.7), quando há a chegada de mensagens em um nó apenas, nota-se um comportamento não-linear (Figuras 5.22a e 5.25a). No início da curva há um crescimento mais rápido, enquanto na sequência, um crescimento mais lento. Já no caso de chegada de mensagens em nós aleatórios, este comportamento não é percebido (Figuras 5.22b e 5.25b). As causas deste comportamento deverão ser investigadas em trabalhos futuros.

Nos gráficos que mostram os resultados em que o consumo da força de atração nos nós é linear possuem curvas mais próximas dos resultados ideais (Figuras 5.20 a 5.25). Nestas curvas, também se observa o comportamento anormal no caso de reputações com crescimento linear (Figura 5.7). Nestas simulações percebe-se também que os picos ficam limitados a 20 mensagens, pois após este número mensagens, consumindo 5% de força de atração cada, a força do nó chega a zero (Figura 5.25a). Principalmente para os casos de menor reputação do consumo linear de força, houve casos identificados de falha no roteamento de mensagens, na ordem de 0,5% dos casos no pior cenário. Estes casos foram removidos da amostra e substituídos por dados válidos obtidos em outras execuções da mesma simulação. Em trabalhos futuros estes casos devem ser analisados.

Houve falhas de roteamento também nas simulações básicas, nos dois modelos, nos casos de reputação média mais próxima de 100%. No pior caso aproximadamente 1% das simulações sofreram este problema, e foram substituídas por dados válidos. Após análise, detectou-se que esta falha é reproduzida mesmo que não haja mudanças no código base do simulador.

Ao analisar o gráfico com ordenação por *ranking* (Figura 5.26), é possível notar mais visivelmente a diferença entre os modelos transitivo e não-transitivo. Enquanto o modelo não-transitivo tem sua curva se aproximando rapidamente do resultado ideal (distribuição média de exatamente 10 mensagens por nó), o modelo não-transitivo tem uma aproximação mais lenta deste ideal. Observa-se que no caso em que todos os nós possuem 50% de reputação a distribuição de ambos é muito similar. O modelo não-transitivo demonstra uma performance melhor de distribuição entre 50% e 100% de reputação, quando ambas as curvas voltam a se unir. É possível inferir a causa do modelo não-transitivo possuir um resultado próximo do perfeito quando as reputações são todas 85%. Neste

caso, a redução da força de atração causada pela reputação é de 15%, enquanto a redução da força causada pelo recebimento de mensagens é de 20%. Como o modelo não-transitivo traz uma visão quase uniforme (exceto pelo narcisismo) das forças dos nós no plano, a reputação perde o seu efeito se comparado com todos os nós com 100% de reputação. Isto na verdade é uma vantagem em relação ao modelo transitivo, pois é um resultado mais próximo do ideal.

5.7 Conclusão

Neste capítulo foram apresentadas duas maneiras de aplicação de reputação em redes magnéticas virtuais. Foram apresentados experimentos utilizando estes dois métodos e o processo de pesquisa necessário para atingir estes objetivos. Na sequência resultados de diversos experimentos foram exibidos, variando curvas de reputação, a metodologia de como as mensagens são entregues e maneira de consumo de força de atração dos nós. Ao final estes resultados foram analisados.

Pode-se perceber, a partir das análises, que um dos principais fatores que influenciam os resultados foi o narcisismo dos nós. É claro também que a conectividade alta dos experimentos aproximou os resultados dos modelos transitivo e não-transitivo, mas pode-se notar claramente a diferença de distribuição de mensagens entre os dois modelos nas simulações realizadas com reputação idêntica para todos os nós. Pode-se notar a vantagem do modelo não-transitivo, que possui melhor distribuição mesmo sendo influenciado pelo narcisismo dos nós.

Ao final, pode-se concluir que ambos os modelos oferecem soluções viáveis para a mitigação do problema de nós mal intencionados ou defeituosos em uma rede magnética virtual. Enquanto o modelo transitivo é mais adequado para situações em que o caminho de roteamento de mensagens deva ser o mais confiável possível, o modelo não-transitivo se preocupa mais com a confiabilidade do nó destino da mensagem.

Capítulo 6

Conclusão

Este trabalho apresentou uma solução completa para o problema de nós maliciosos ou defeituosos que aumentam artificialmente sua força de atração em redes magnéticas virtuais. Optou-se pelo uso do EigenTrust para ponderar as ações maliciosas dos nós, pois provê uma maneira matematicamente confiável de se obter reputações globais dos nós.

Como uma primeira contribuição, foi proposta a otimização do EigenTrust com a substituição de DHTs por redes magnéticas virtuais para a escolha do *Score Manager*, o que provou-se analiticamente que traz benefícios indiscutíveis na hora de busca por *Score Managers*, por ser um algoritmo pró-ativo, enquanto se mostrou escalável e sem grandes compromissos de performance no caso de entrada e saída de nós. Sendo assim, esta substituição traz ganho real no desempenho médio da rede que utiliza EigenTrust como sistema de confiança e reputação.

A segunda contribuição foi a proposta de, em Redes Magnéticas Virtuais, uma metodologia para estabelecimento de topologia de planos com entrada e saída de nós de forma dinâmica sem, no entanto, have particionamento do plano. Esta metodologia, por mais que tenha sido proposta no contexto de escolha de *Score Managers* no EigenTrust, se mostra aplicável não só neste caso, mas também em casos genéricos de uso de redes magnéticas virtuais.

Tendo estabelecida uma arquitetura que permite a obtenção de valores de reputação globais para os nós em um plano magnético virtual, a terceira contribuição apresentou duas metodologias de aplicação de reputação em redes magnéticas virtuais. Diversas simulações foram realizadas utilizando os dois modelos, sendo eles o transitivo, em que a força de atração é ponderada pela reputação do nó em cada mensagem de propagação trocada, e o não-transitivo, em que as mensagens são transmitidas com forças sem ponderação e a reputação é levada em conta para a escolha do pivô. Conclui-se que ambos os modelos oferecem soluções viáveis para a mitigação do problema proposto. O modelo

transitivo se mostra mais apropriado em situações em que o caminho de roteamento de mensagens deva ser o mais confiável possível, por considerar a reputação de todos os nós no caminho até o pivô para o cálculo de forças. O modelo não-transitivo é mais focado na confiabilidade do nó destino da mensagem, independente do caminho que a mensagem faça para chegar a este destino. Como esperado, o modelo não-transitivo mostrou resultados mais próximos do ideal, por ignorar a reputação dos nós por onde a mensagem transita. Caso a aplicação permita, o uso de entrega de mensagens diretamente ao pivô pode ser uma solução para evitar caminhos contendo nós maliciosos, usando a rede magnética virtual como mecanismo de descoberta somente, permitindo usar o modelo não-transitivo sem risco de obter um caminho não confiável.

Como trabalho futuro é proposta a realização de simulações do uso de redes magnéticas virtuais para a escolha do *Score Manager* no EigenTrust, assim como a otimização desta proposta. Outro trabalho futuro é a realização de mais simulações para entender de forma mais clara alguns comportamentos dos modelos transitivo e não-transitivo constatados nas simulações realizadas. Outro trabalho futuro possível é a alteração da fórmula da maneira com que a força de atração é ponderada pela reputação de um nó. Finalmente, uma implementação real do sistema proposto pode ser realizada.

Referências Bibliográficas

BRIN, S. et al. The PageRank citation ranking: bringing order to the web. In: *Proceedings of ASIS'98*. [S.l.: s.n.], 1998. p. 161–172.

CALSAVARA, A.; LIMA JR., L. Routing Based on Message Attraction. In: IEEE. *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*. [S.l.], 2010. p. 189–194.

CASTELFRANCHI, C.; FALCONE, R. Social trust: A cognitive approach. *Trust and deception in virtual societies*, Citeseer, p. 55–90, 2002.

CLAESSENS, J.; PRENEEL, B.; VANDEWALLE, J. (How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions. *ACM Transactions on Internet Technology (TOIT)*, ACM, v. 3, n. 1, p. 28–48, 2003.

FIPS, P. 180-2: Secure Hash Standard. *US Department of Commerce, Technology Administration, National Institute of Standards and Technology*, 2002.

FREEMAN, L. Centrality in social networks. *Social Networks*, v. 1, n. 3, p. 215–239, 1979.

GAMBETTA, D. Can we trust. *Trust: Making and Breaking of Cooperative Relations, New York, Basil Blackwell*, p. 213–238, 1988.

JøSANG, A.; ISMAIL, R.; BOYD, C. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, Elsevier, v. 43, n. 2, p. 618–644, 2007.

KAMVAR, S.; SCHLOSSER, M.; GARCIA-MOLINA, H. The eigentrust algorithm for reputation management in p2p networks. In: ACM. *Proceedings of the 12th international conference on World Wide Web*. [S.l.], 2003. p. 640–651.

LIMA JR., L.; CALSAVARA, A. Autonomic Application-Level Message Delivery Using Virtual Magnetic Fields. *Journal of Network and Systems Management*, Springer, v. 18, n. 1, p. 97–116, 2010.

MARSDEN, P.; LIN, N. *Social structure and network analysis*. [S.l.]: Sage Beverly Hills, CA, 1982.

MCKNIGHT, D.; CHERVANY, N. The meanings of trust. *Trust in Cyber-Societies-LNAI*, Citeseer, v. 2246, p. 27–54, 2001.

STUTZBACH, D.; REJAIE, R. Understanding churn in peer-to-peer networks. In: ACM. *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. [S.l.], 2006. p. 189–202. ISBN 1595935614.

WANG, Y.; VASSILEVA, J. Trust and reputation model in peer-to-peer networks. In: CITESEER. *Proceedings of the 3rd International Conference on Peer-to-Peer Computing*. [S.l.], 2003. p. 150.

WATTS, D.; STROGATZ, S. Collective dynamics of 'small-world' networks. *Nature*, Nature Publishing Group, v. 393, n. 6684, p. 440–442, 1998.

XIONG, L.; LIU, L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering*, v. 16, n. 7, p. 843–857, 2004.

YAU, P.; MITCHELL, C. Reputation methods for routing security for mobile ad hoc networks. In: *Mobile Future and Symposium on Trends in Communications, 2003. SympoTIC'03. Joint First Workshop on*. [S.l.: s.n.], 2003. p. 130–137.