Análise matemática para avaliação de desempenho em ambientes *Peer-to-Peer*

Érico Santos Rocha[1], Janaina Lemos[1], Daniel Bertoglio[1], Rafael Ávila[1], Luis Paulo Luna de Oliveira[1]

[1]PIPCA - Programa de Pós-Graduação em Computação Aplicada
Universidade do Vale do Rio dos Sinos(UNISINOS)
São Leopoldo – RS – Brasil

{ericomsr, janaina.lemos, dalalana}@gmail.com, {rbavila, lpluna}@inf.unisinos.br

Resumo. *A utilização da tecnologia P2P tem crescido consideravelmente nos últimos anos, sendo tema de diversas pesquisas. Dentre as inúmeras vertentes de estudo destacam-se as questões relacionadas com o desempenho deste ambiente após o emprego de mecanismos de segurança. Este artigo apresenta uma análise matemática com o uso de equações diferenciais para os modelos de comunicação cliente-servidor, P2P e P2P com o uso de criptografia, avaliando o comportamento destes cenários com relação a utilização e disponibilidade de recursos.*

1. Introdução

Nos últimos anos os trabalhos de pesquisa direcionados aos sistemas *Peer-to-Peer* (P2P) aumentaram de forma expressiva. Esta tecnologia proporciona conectividade em larga escala e possibilita o aproveitamento de recursos como processamento e capacidade de armazenamento das máquinas participantes da rede, uma vez que cada nodo pode atuar como cliente, servidor ou ambos. Estes fatos tornam esta tecnologia um elemento importante dentro da computação distribuída.

Com a popularização da tecnologia P2P em ambientes acadêmicos e corporativos, cresce também a necessidade do uso de mecanismos de segurança neste tipo de rede, de modo que evite ações maliciosas de seus componentes, aumentando significativamente o interesse dos pesquisadores por este campo.

Este trabalho tem como objetivo avaliar com o uso de modelos matemáticos o comportamento de três diferentes cenários em relação à disponibilidade e utilização de recursos. No primeiro cenário tem-se a topologia tipo estrela, onde o servidor é o ponto central e as máquinas clientes são as extremidades. O segundo é constituído por uma rede P2P. Já no terceiro e último cenário é incorporado o uso de recursos criptográficos na rede apresentada no cenário 2, visando avaliar o impacto causado pela inclusão de tais recursos no sistema.

É apresentado o modelo matemático com equações diferenciais para representar a relação entre a disponibilidade e a utilização de recursos em uma rede com um servidor e n clientes (cenário 1). Para os cenários seguintes foram realizadas modificações nesse modelo, de forma a atender as premissas que regem a troca de dados dentro do ambiente P2P. O modelo foi construído com o auxílio do software Mathematica.

Este artigo está organizado da seguinte forma, a seção 2 define o modelo, a seção 3 desenvolve as equações do modelo. A seção 4 destina-se a análise e avaliação dos resultados. Na seção 5 encontram-se as considerações finais deste estudo.

2. Definição do modelo

Uma rede *Peer-to-Peer*, é representada pela união lógica de diversos computadores de forma descentralizada. Diferente da topologia tradicional, apresentada na figura 1, em que cada integrante pode atuar apenas como servidor ou cliente, nos ambientes P2P cada membro é capaz de assumir ambas as funções de forma simultânea e com diversos pares.

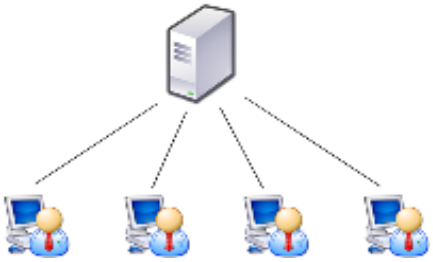

Figura 1: Topologia tradicional de rede

Na comunicação P2P, ilustrada na figura 2, a relação entre cada membro é realizada aos pares, desta forma cada integrante conecta-se aos demais para fornecer ou solicitar serviços. Este conjunto de conexões lógicas resulta em uma rede com topologia fortemente conectada (*full-mesh*) pelo fato de que cada integrante estar apto a formar pares com todos os demais membros da rede.

Figura 2: Comunicação P2P

Entre as diversas aplicações da tecnologia P2P, podem ser citados o compartilhamento de arquivos e os sistemas de armazenamento de arquivos em rede. É cada vez mais comum a utilização desta tecnologia em universidades e empresas, fato que torna necessário o emprego de mecanismos de segurança nestas redes. Por este motivo, será avaliado neste trabalho o impacto causado pela inclusão de recursos criptográficos no modelo matemático proposto. Para tanto, será considerado o uso de criptografia assimétrica, onde os nodos comunicantes utilizam uma chave pública para criptografar os dados e uma chave privada para obter a informação original.

Tendo como base o comportamento mencionado anteriormente, foi desenvolvido modelo matemático com equações diferenciais para permitir a avaliação do consumo e da disponibilidade de recursos na comunicação cliente-servidor. O

conjunto de equações que compõem este modelo tem como origem o modelo presa-predador descrito em Peixoto (2007), no qual a disponibilidade de recursos representa as presas deste sistema e, por conseqüência, o comportamento predatório é dado através da carga de utilização da rede.

A seguir são mostradas algumas definições importantes que serão utilizadas no decorrer deste trabalho.

- Matriz Jacobiana: Matriz formada por derivadas parciais de primeira ordem. É utilizada no estudo do comportamento (ou estabilidade) de sistemas dinâmicos ao redor dos pontos fixos (ponto onde as derivadas são nulas).
- Autovalores da matriz Jacobiana: Fornecem informações relativas a estabilidade local de um determinado ponto fixo.

Maiores informações sobre estes aspectos são encontradas em Anton (2002) e Stewart (2005).

A seguir é apresentado o conjunto de equações para a comunicação cliente-servidor.

$$f1 = a \times (1 - x) + p1 \times (1 - x) \times y$$
$$f2 = b \times (1 - y) - p2 \times (1 - y) \times x$$

Cada termo que forma este conjunto de equações são definidos da seguinte forma:

- $f1$: Taxa de variação da utilização. Este fator define a progressão do grau de ocupação dos recursos disponíveis na rede;
- $f2$: Taxa de variação da disponibilidade. Consiste na variação ao longo do tempo dos recursos que se apresentam ociosos;
- $p1$: Saúde servidor. Constante que representa a confiabilidade do conjunto de nós com a função de servidores;
- $p2$: Saúde cliente. Define o potencial constante (grau de voracidade) dos clientes inseridos no sistema para os recursos a serem consumidos;
- a: Coeficiente de resposta a utilização. Constante que define o fator de crescimento mínimo da utilização do sistema;
- b: Coeficiente de resposta a disponibilidade. Dentro do modelo, esta constante representa a variação mínima da disponibilidade de recursos;
- x: Utilização. Fornece ao modelo a proporção de recursos utilizados a cada instante de tempo. Serve como base para as interações subseqüentes do funcionamento do sistema;
- y: Disponibilidade. De forma análoga a utilização representa os recursos disponíveis;
- $(1 - y)$ e $(1 - x)$: Representam respectivamente a parcela média de recurso indisponível e disponível na rede, com uma taxa variando de 0 a 100% dos recursos.

No que tange a comunicação P2P, o modelo cliente-servidor, foi modificado visando atender as especificações que definem o novo método de comunicação em

análise. O novo conjunto de equações que modelam a comunicação P2P é apresentado abaixo.

$$f1 = a \times (1 - x^2) + p1 \times (1 - x^2) \times y^2$$
$$f2 = b \times (1 - y^2) - p2 \times (1 - y^2) \times x^2$$

Em virtude da comunicação P2P não garantir um equilíbrio entre o percentual de nós que atuam como servidor ou cliente desta rede, definiu-se que os termos que trata diretamente a disponibilidade de recursos deveriam ser elevados ao quadrado para caracterizar a modelagem deste ambiente de comunicação. Esta definição baseia-se no fato de que em grandes ambientes P2P a quantidade de nós em conjunto de suas funções exercerão baixo impacto neste equilíbrio. Um nó será cliente de determinado conteúdo e servidor de outros, conforme Barcellos (2006), logo a tendência deste equilíbrio passa a ser um fator natural e, portanto, reforça as alterações apresentadas anteriormente.

Como já foi mencionado, este estudo visa avaliar o comportamento do sistema quando são aplicadas técnicas de segurança ao mesmo. Para atingir este objetivo, foi acrescentada a componente criptográfica **c** ao conjunto de equações para a comunicação P2P. Esta componente está diretamente relacionada ao tamanho em bits da chave criptográfica aplicada. O menor valor admitido para **c** é **1,** indicando que não esta sendo utilizada a criptografia. A seguir é apresentado o conjunto de equações resultantes da aplicação do coeficiente **c**.

$$f1 = (a \times (1 - x^2) + p1 \times (1 - x^2) \times y^2) \times \mathrm{c}$$
$$f2 = (b \times (1 - y^2) - p2 \times (1 - y^2) \times x^2) \times \mathrm{c}$$

3. Desenvolvimento

A partir do modelo proposto para cada cenário, foram efetivados os cálculos necessários para execução da analise entre os ambientes. A seguir apresentados o cálculo das singularidades, matriz Jacobiana correspondente bem como os autovalores para os cenários propostos. Os cálculos foram feitos no software Mathematica.

A seguir são apresentados os pontos singulares para o cenário 1, que compreende o Modelo cliente-servidor:

$$\left\{\{x \to 1, y \to 1\}, \left\{x \to \frac{b}{p2}, y \to -\frac{a}{p1}\right\}\right\}$$

A matriz Jacobiana para o cenário 1 é mostrada a seguir:

$$\begin{pmatrix} -a - p1y & p1(1-x) \\ -p2(1-y) & -b + p2x \end{pmatrix}$$

Abaixo, são mostrados os autovalores para o cenário 1 – Modelo cliente-servidor

$$\{-a - p1, -b + p2\}$$

A seguir, são mostrados os cálculos realizados para o cenário 2, onde tem-se o Modelo P2P.

Os pontos singulares para o cenário 2 são mostrados abaixo:

$$\{\{x \to -1, y \to -1\},\ \{x \to -1, y \to 1\},\ \{x \to 1, y \to -1\},\ \{x \to 1, y \to 1\},\ \left\{x \to -\frac{\sqrt{b}}{\sqrt{p2}}, y \to -\frac{i\sqrt{a}}{\sqrt{p1}}\right\},$$
$$\left\{x \to -\frac{\sqrt{b}}{\sqrt{p2}}, y \to \frac{i\sqrt{a}}{\sqrt{p1}}\right\},\ \left\{x \to \frac{\sqrt{b}}{\sqrt{p2}}, y \to -\frac{i\sqrt{a}}{\sqrt{p1}}\right\},\ \left\{x \to \frac{\sqrt{b}}{\sqrt{p2}}, y \to \frac{i\sqrt{a}}{\sqrt{p1}}\right\}\}$$

A seguir, a matriz Jacobiana gerada para o cenário 2:

$$\begin{pmatrix} -2ax - 2p1xy^2 & 2p1(1-x^2)y \\ -2p2x(1-y^2) & -2by + 2p2x^2y \end{pmatrix}$$

Por último, os autovalores para o cenário 2:

$$\{-2(a+p1), -2b + 2p2\}$$

No terceiro cenário é incluído o uso de criptografia a rede P2P proposta no cenário 2.

Os pontos singulares para o cenário 3 – Modelo P2P com criptografia são apresentados abaixo:

$$\left\{\{x \to -1, y \to -1\},\ \{x \to -1, y \to 1\},\ \{x \to 1, y \to -1\},\ \{x \to 1, y \to 1\},\ \left\{x \to -\frac{\sqrt{b}}{\sqrt{p2}}, y \to -\frac{i\sqrt{a}}{\sqrt{p1}}\right\},\right.$$
$$\left.\left\{x \to -\frac{\sqrt{b}}{\sqrt{p2}}, y \to \frac{i\sqrt{a}}{\sqrt{p1}}\right\},\ \left\{x \to \frac{\sqrt{b}}{\sqrt{p2}}, y \to -\frac{i\sqrt{a}}{\sqrt{p1}}\right\},\ \left\{x \to \frac{\sqrt{b}}{\sqrt{p2}}, y \to \frac{i\sqrt{a}}{\sqrt{p1}}\right\}\right\}$$

A seguir, matriz Jacobiana para o cenário 3:

$$\begin{pmatrix} c(-2ax - 2p1xy^2) & 2cp1(1-x^2)y \\ -2cp2x(1-y^2) & c(-2by + 2p2x^2y) \end{pmatrix}$$

Abaixo, os autovalores gerados para o cenário 3:

$$\{-2c(a+p1), -2c(b-p2\}$$

Para a definição dos autovalores, foram analisados apenas os pontos singulares onde as componentes x e y proporcionassem valores positivos. Esta definição se deve a natureza das taxas tratadas pelo modelo não permitindo valores negativos para a disponibilidade e utilização.

Desta forma para os três cenários em analise apenas a singularidade dada por $x = 1$ e $y = 1$ será avaliada.

4. Analise e avaliação dos resultados

De acordo com todas as premissas observadas anteriormente, juntamente com as equações do modelo e suas resultantes (singularidades e autovalores), conclui-se que a variação das taxas f1 e f2 são influenciadas pelas constantes a, b e p1.

Adicionalmente, os termos $\boldsymbol{p1 \times (1-x) \times y}$ e $\boldsymbol{p2 \times (1-y) \times x}$, que representam o encontro entre disponibilidade e utilização do sistema colaboram para a queda da taxa de disponibilidade dada por f1 e conseqüentemente para a elevação da taxa de utilização resultante de f2. Desta forma é possível confirmar a premissa que define apenas valores positivos para as constantes **p1** e **p2**. Caso este assuma o valor

zero a relação entre a taxa de ocupação e disponibilidade deixará de existir, caracterizando desta forma um comportamento inexistente em redes P2P.

Partindo das premissas e constatações realizadas até o ponto atual deste estudo, os seguintes cenários foram avaliados em torno da singularidade $\{x = 1, y = 1\}$:

a) $\{x = 1, y = 1\}, a = b = 0, p1 = p2 > 0$

Nesta situação, as parcelas $b \times (1 - y^2)$ e $a \times (1 - x^2)$ pertencentes respectivamente a f1 e f2 não exercem qualquer influência nas taxas do sistema. Esta responsabilidade pertence exclusivamente a saúde do servidor dada por ***p1*** e a saúde dos clientes dada por ***p2***, tendo como resultando um sistema ponto de sela com atração em x e repulsão em y. A figura 3 ilustra este comportamento.

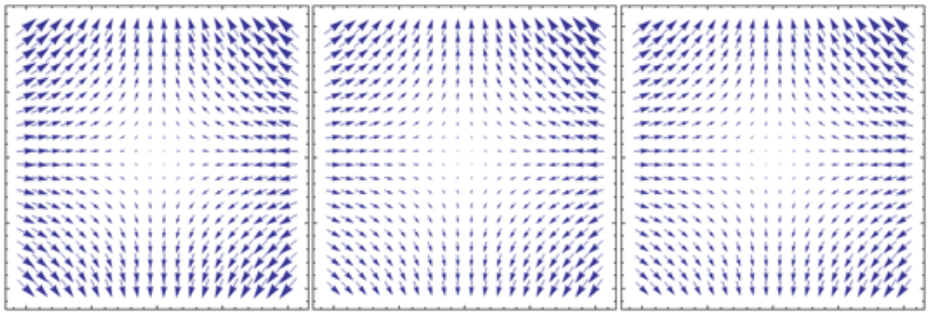

Figura 3: Singularidade {x=1,y=1}, a=b=0,c=1, p1=p2 > 0

b) $\{x = 1, y = 1\}, a > b = 0, c = 1, p1 = p2 > 0$

Neste cenário, f2 sofrerá influência do coeficiente de resposta a utilização, desta forma a utilização crescerá com maior taxa de variação em relação a disponibilidade. O sistema continuará apresentando um comportamento sela em torno do ponto singular, mas de forma desequilibrada, com f2 exercendo maior força de repulsão do que f1 exerce em atração.

c) $\{x = 1, y = 1\}, a = 0, b > 0, c = 1\ p1 = p2 > 0$

O resultado proporciona a f1 maior crescimento em relação à f2. O modelo apresenta a formação de sela ao redor do ponto fixo com desequilíbrio contrário ao apresentado no passo anterior.

d) Variação da Saúde dos servidores e clientes (**p1,p2**)

A constante **p1** é um fator positivo ao sistema, afetando a taxa de variação de disponibilidade **f1**, ou seja, quanto mais próxima de 0 menor será esta variação resultando assim na ocupação e desocupação mais vagarosa de um servidor da rede. Este comportamento esta em total acordo com o funcionamento de uma rede P2P, pois nesta cada integrante é pontuado de acordo com diversos critérios (Processamento, velocidade de conexão, quantidade de arquivos para oferecer, etc.).

No ingresso inicial de um membro a rede sua pontuação é baixa, pois estes dispõem de poucos arquivos para oferecer e a medida que sua base de arquivos vai aumentando, sua ocupação aumenta vagarosamente até seu respectivo ponto de saturação de recursos, ocasionando assim a queda vagarosa de conexões a este servidor.

Quanto mais próximo de 1 estiver a saúde do servidor significa que mais recursos este dispõe a oferecer. Em comparação ao mundo real, isto pode ocorrer quando um determinado host deixa à rede P2P A para ingressar na rede B; ao ingressar nesta, ele já dispõe de diversos recursos obtidos na primeira participação, logo sua saúde será maior e a procura por arquivos neste membro ocorrerá de forma mais acentuada. De forma análoga, a constante **p2** é um fator que influencia a taxa de variação de utilização **f2**. Conforme **p2** se aproxima de 0, menor será a taxa de variação **f2**. Isto significa que a ocupação dos recursos dos servidores da rede ocorrerá de forma mais lenta.

e) Comparação entre os cenários propostos. Tradicional e P2P.

Quando comparado ao modelo tradicional de comunicação, o modelo P2P apresenta variação acelerada de suas respectivas taxas. Este comportamento é obtido devido ao sistema de conexões por meio de pares que o P2P oferece. Se um arquivo esta disponível em várias fontes, a resposta do sistema a uma requisição tenderá a ser mais rápida justamente por não existir ponto central de conexão. Ao incorporar ao modelo recursos criptográficos percebe-se pequena variação no desempenho do sistema, mesmo quando a componente criptográfica assume valores elevados, indicando que o emprego destas técnicas é vantajosa devido ao ganho de segurança proporcionado.

5. Considerações finais

O modelo apresentado teve como objetivo principal possibilitar a análise matemática do comportamento dos recursos quanto a sua utilização e disponibilidade em diferentes cenários. Os resultados mostram que um ambiente *Peer-to-Peer* apresenta ganho de desempenho significativo mesmo com a aplicação de mecanismos de segurança, no caso, a criptografia simétrica. Estes resultados subsidiam a continuidade dos trabalhos no sentido de projetar e desenvolver um sistema destinado ao compartilhamento P2P em redes locais.

6. Referências

Stewart, J. *Cálculo*. Pioneira, Vol. 2, 5ª ed., 2005.

Anton, H. *Cálculo, Um novo horizonte*. Bookman, Vol. 2, 6 ª ed., 2002.

Dawkins, P. *Calculus III.* Disponivel em: http://tutorial.math.lamar.edu/dowload.aspx?PDF=B,11;11. Acessado em 13 de junho de 2009

Peixoto, M.S., Barros, L.C., Bassanezi, R.C. Uma Abordagem Fuzzy para um Modelo Presa-predador Acoplado ao Parasitismo. Disponível em: http://www.sbmac.org.br/tema/seletas/docs/v8_1/13-Peixoto.pdf. Acesso em 10 de agosto de 2009

Barcelos, M.P., Gaspary, L.P, Fundamentos, Tecnologias e Tendências rumo a Redes P2P Seguras. Disponível em: http://www.sbc.org.br/bibliotecadigital/download.php?paper=640. Acesso em 10 de agosto de 2009