



PROPOSTA DE TRABALHO DE CONCLUSÃO

IDENTIFICAÇÃO

ALUNO Giovani Facchini		MATRÍCULA 0884997-8	
CURSO Ciência da Computação			
ENDEREÇO Rua Coronel Flores, 2361			
BAIRRO Centro		CIDADE Taquara	UF RS
CEP 95600-000	FONE (51) 84271421	E-MAIL facchini@gmail.com	

PROPOSTA DE DESENVOLVIMENTO

ORIENTADOR Marinho Pilla Barcellos			
TÍTULO DO TRABALHO Escalabilidade, autonomia e segurança em redes Peer-to-Peer: repensando a P2PSL			
PALAVRAS-CHAVE	Peer-to-Peer	Segurança	Sistemas Distribuídos

MOTIVAÇÃO

Em maio de 1999, Shawn Fanning, criou o primeiro sistema de troca de arquivos P2P (peer-to-peer) – Napster [1]. O Napster permitiu que usuários (chamados peers) pudessem baixar cópias de músicas no formato MP3 para seus PC's. Em um ano o número de usuário passou de 50 milhões e com isso deu-se o início de uma nova era onde o paradigma tradicional cliente/servidor sofre um grande impacto.

Com a popularidade do Napster muitas aplicações para compartilhamento de arquivos foram criadas. Entre essas aplicações pode-se citar KaZaA e eMule que são amplamente utilizados ainda hoje. Com esse novo paradigma (P2P) a pesquisa se volta para essa área criando novos protocolos de busca de dados, formas de compartilhamento anônimo de informação, mecanismos de gerência de reputação e incentivo à cooperação, esquemas para gerência de confiabilidade e aspectos de segurança.

Muitas publicações foram feitas nessa área conceituando tipos de redes e estruturas, formas de comunicação, novos protocolos e segurança. Nessa conceituação, define-se uma rede P2P como sendo uma rede overlay [2] configurada sobre a rede IP formando uma rede lógica independente da rede física de forma que os nodos fiquem interconectados e troquem informações diretamente sem a necessidade de um servidor central.

Como descrito em [3], as redes P2P foram classificadas em dois grupos. O primeiro deles representa as primeiras redes P2P criadas e chama-se “Não Estruturado”. Esse modelo conecta os peers em um grafo ramdomico e utiliza como sistema de busca modelos de *flooding*, *random walks* ou *expanding-ring TTL search*. O outro modelo é o Estruturado. Neste, cada peer que se conecta ao sistema recebe um ID único no sistema identificando o mesmo.

Cada objeto é representado por uma chave e fica sob a responsabilidade de um (ou mais de um) determinado peer. Dessa forma, algoritmos de roteamento podem descobrir o detentor de um objeto de maneira mais eficiente (normalmente $O(\log N)$).

Hoje existe uma vasta gama de aplicações baseadas em P2P como troca de arquivos, programas de mensagens instantâneas, processamento colaborativo, compartilhamento de recursos, entre outros. O grande problema atual acontece porque todos esses ambientes foram concebidos sem uma visão voltada para segurança computacional. Com isso, muitos ataques podem ser feitos a uma rede como negação de serviço, poluição de conteúdo, censura a documentos, violação de anonimato, partições de rede, entre outros.

Para oferecer requisitos de segurança de uma rede P2P, em [4] é proposta uma camada de segurança que permite flexibilidade na escolha e uso de mecanismos de segurança, de acordo com os requisitos da aplicação. Em [5] é descrito um cenário de avaliação da ferramenta, denominada P2PSL, e junto com isso um protocolo para troca de chaves. Apesar de modular, a ferramenta foi baseada na existência de uma topologia de rede mais ou menos estável e de tamanho limitado, sendo executada sobre JXTA [6] e OurGrid [7]. Essa ferramenta também assume relativa confiança (*trust*) nos nodos.

OBJETIVOS

Este trabalho tem como objetivo endereçar as questões acima, repensando a P2PSL em função de aspectos típicos de redes P2P atuais: escalabilidade, taxa de “churn”, ou seja, entrada e saída frequente de nodos (incluindo falhas) e autonomia dos nodos.

Como consequência, será feita uma análise quanto à camada subjacente, provavelmente levando à substituição da infra-estrutura atual (JXTA) por uma solução baseada em DHT (Distributed Hash Table), tal como Chord.

Os critérios utilizados nesta análise serão, particularmente, escalabilidade (complexidade de tempo e comunicação) e grau de resistência a ataques.

METODOLOGIA

A execução do trabalho pode ser definida nas seguintes etapas:

1. Estudo do estado da arte na área de P2P e segurança, enfatizando estruturas, algoritmos, vantagens e desvantagens de cada esquema
2. Estudo de modelos de redes P2P propostos e implementados, escolhendo um para integrar o modelo e a camada de segurança P2PSL
3. Integrar a camada de segurança P2PSL com o modelo de rede P2P escolhido
4. Estudar algoritmos para gerência de chaves criptográficas em redes P2P
5. Implementar o algoritmo escolhido
6. Testar e avaliar o novo ambiente composto, empregando as métricas anteriormente descritas

7. Redação da monografia

CRONOGRAMA

As etapas citadas na metodologia estão previstas de acordo com o cronograma a seguir. Os números 1 à 7 correspondem às atividades descritas na seção anterior.

	<i>Mar</i>	<i>Abr</i>	<i>Mai</i>	<i>Jun</i>	<i>Jul</i>	<i>Ago</i>	<i>Set</i>	<i>Out</i>	<i>Nov</i>
1									
2									
3									
4									
5									
6									
7									

BIBLIOGRAFIA

- [1] **NAPSTER**. Março 2006. <http://www.napster.com>
- [2] Lua, Eng K.; Crowcroft, Jon; Pias, Marcelo. **A Survey and Comparison of Peer-to-Peer Overlay Network Schemes**. IEEE Communications Surveys & Tutorials. Second Quarter 2005.
- [3] Theotokis, S.A.; Spinellis, D. **A Survey of Peer-to-Peer Content Distribution Technologies**. ACM Computing Surveys, Vol. 36, No. 4, December 2005, pg 335-371.
- [4] Detsch, André. **Uma Arquitetura para Incorporação Modular de Aspectos de Segurança em Aplicações Peer-to-Peer**. Dissertação de Mestrado. Unisinos 2005.
- [5] Detsch, André; Gaspary, L. P.; Barcellos, M. P.; Sanchez, R. N. **Flexible Security Configuration & Deployment in Peer-to-Peer Applications**. NOMS 2006. April 2006.
- [6] **JAL - JXTA Abstraction Layer**. Março 2006. <http://ezel.jxta.org/jal.html>
- [7] N. Andrade, W. Cirne, F. V. Brasileiro, P. Roisenberg, "OurGrid: An Approach to Easily Assemble Grids with Equitable Resource Sharing", em Job Scheduling Strategies for Parallel Processing, 9th International, workshop JSSP 2003, pags. 61-86, June 2003.

AVALIADORES

1. Luciano Paschoal Gaspary
2. Gerson G. H. Cavalheiro
3. Valter Roesler
4. Lisandro Zambenedetti Granville (UFRGS)

DATA

10/03/2006

ALUNO

ORIENTADOR