Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Roberto Costa Flores

REDES PEER-TO-PEER:
Um estudo sobre aspectos de segurança e mobilidade

Rio de Janeiro

2005

Roberto Costa Flores

REDES PEER-TO-PEER:
Um estudo sobre aspectos de segurança e mobilidade

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Profa. Luci Pirmez, D. Sc., COPPE/UFRJ, Brasil

Rio de Janeiro

2005

Roberto Costa Flores

REDES PEER-TO-PEER:
Um estudo sobre aspectos de segurança e mobilidade

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em dezembro de 2005

Profa. Luci Pirmez, D. Sc., COPPE/UFRJ, Brasil

Dedico este trabalho às pessoas mais importantes de minha vida: meus pais, irmãos e amigos. E, logicamente, à Alessandra.

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, pelo seu amor e apoio incondicional em todos os momentos de minha vida. Sem eles, nada seria possível. Nada teria sentido.

À Alessandra, por toda a ajuda, amor e compreensão dados ao longo desse tempo. Foi igualmente fundamental para o meu êxito.

Aos meus irmãos, pelo apoio que me deram durante toda a minha vida.

RESUMO

FLORES, Roberto Costa. **REDES PEER-TO-PEER: Um estudo sobre aspectos de segurança e mobilidade.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

Os estudos sobre as redes P2P começaram na década de 80, quando foi identificada a possibilidade de compartilhamento direto de arquivos e informações sem a necessidade de um elemento central, além da possibilidade real de compartilhamento de recursos computacionais, como por exemplo memória e espaço em disco.

A partir deste momento, importantes projetos começaram a ser desenvolvidos, como por exemplo o Napster, SETI@home, Gnutella e Jabber. Com isso, usuários localizados nos mais distantes pontos da Internet passaram a conseguir trocar informações diretamente, formando grandes comunidades na rede sem a necessidade de um servidor central.

Entretanto, com o passar do tempo, aconteceram problemas na utilização das redes e sistemas P2P. Um deles foi relativo às questões de direitos autorais (copyright), o que reduziu consideravelmente a utilização de sistemas de compartilhamento de arquivos, como por exemplo o Napster, que permitia a troca de músicas entre os usuários de forma ilegal.

Uma outra questão importante e atual refere-se ao aspecto de segurança nas redes P2P. Algumas características destes sistemas os deixam muito vulneráveis a ataques por parte de usuários mal intencionados, que podem gerar danos simples a usuários domésticos e até mesmo grandes fraudes em corporações, acarretando em grandes perdas de receita. Por isso, existe cada vez mais uma preocupação com os processos internos destes sistemas, como por exemplo controles de conexão, autenticação e operação dos mesmos.

A grande utilização de dispositivos móveis atualmente já está gerando novas tendências nos sistemas P2P. Novos aplicativos já estão em desenvolvimento para atender a este aspecto de mobilidade, como por exemplo o *"PocketSkype"* (transmissão de voz sobre protocolo IP através de um *pocket* PC) e o *"MobileMule"* (compartilhamento de arquivos através do uso de aparelhos celulares).

Desta forma, este trabalho descreve as características das redes e sistemas P2P, considerando as preocupações relativas aos aspectos de segurança, bem como analisando as novas tendências vinculadas aos aspectos de mobilidade.

ABSTRACT

FLORES, Roberto Costa. **PEER-TO-PEER NETWORKS: A study of security and mobility issues.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2005.

The P2P networks researches had started in the beginning of the 80's, when new possibilities for files and resources sharing between different computers were identified, without a need of a central server. For example, sharing of memory and disk space.

From this moment, new important projects were developed, like Napster, SETI@home, Gnutella and Jabber. Users from different places at Internet were able to change informations directly, making communities in the Internet without a need of a central server.

However, the use of P2P networks and systems brought some problems. One of them was related to copyright issues, problem that reduced the use of file-sharing systems. For example Napster, who allowed users to change music files in a illegal way.

Another important and present issue is related to security aspects. Some characteristics of these systems make them vulnerables of bad users attacks. It can cause just few damages to home users or big injuries to large companies, resulting in revenue loses. For this reason, there are a lot of concerns about internal processes in P2P systems, like connection control, authentication and operation issues.

The use of mobile devices nowadays is resulting in new tendencies for P2P systems. New systems have been developed due to this tendencies, like *"PocketSkype"* (voice over IP protocol transmission, through a *pocket* PC) and *"MobileMule"* (file sharing through cell phones).

This work describes the P2P networks and systems characteristics, considering the concerns about security issues and analysing the new tendencies related to mobile aspects.

LISTA DE FIGURAS

Página

Figura 1 – Arquitetura do Napster 24

Figura 2 – Diferenças entre Napster e Gnutella 27

LISTA DE QUADROS

Página

Quadro 1 – Quadro de Descriptors 26

LISTA DE ABREVIATURAS E SIGLAS

P2P	Peer-to-peer
TI	Tecnologia da Informação
IP	Internet Protocol
ATM	Asynchronous Transfer Mode
PSTN	Public Switched Telephone Network
LAN	Local Area Network
DHT	Distributed Hash Table
API	Application Programming Interface
XML	EXtensible Markup Language

SUMÁRIO

	Página
1 **INTRODUÇÃO**	12
1.1 MOTIVAÇÕES	12
1.2 CONCEITO DE P2P	13
1.3 TRABALHOS RELACIONADOS	13
1.4 OBJETIVOS	14
1.5 ORGANIZAÇÃO	14
2 **CONCEITOS BÁSICOS**	15
2.1 INTRODUÇÃO	15
2.2 REDES P2P E REDES OVERLAY	17
2.3 CLASSIFICAÇÃO DOS MODELOS DE ARQUITETURA P2P	17
2.4 DESCENTRALIZAÇÃO EM SISTEMAS P2P	21
2.5 APLICAÇÕES P2P	22
2.5.1 **Compartilhamento de Arquivos**	22
2.5.1.1 Napster	23
2.5.1.2 Gnutella	24
2.5.1.3 Freenet	27
2.5.1.4 KaZaA	28
2.5.1.5 Outras Aplicações	28
2.5.2 **Troca de Mensagens**	29
2.5.2.1 MSN Messenger	29
2.5.2.2 Yahoo! Messenger	29
2.5.2.3 Outras aplicações IM	30
2.5.3 **Outros Projetos P2P**	30
2.5.3.1 SETI@home	30
2.5.3.2 Jabber	31
2.6 PLATAFORMAS DE DESENVOLVIMENTO P2P	32
2.6.1 **JXTA**	32
2.6.2 **.NET**	34
2.6.3 **Groove Development Kit (GDK)**	35
3 **ASPECTOS DE SEGURANÇA EM REDES P2P**	36
3.1 INTRODUÇÃO	36
3.2 PROBLEMAS	36
3.2.1 **Ameaças Externas**	36
3.2.1.1 Roubo	37
3.2.1.2 Obstrução da largura de banda e compartilhamento de arquivo	37
3.2.1.3 Bugs	37
3.2.1.4 Quebra de Criptografia	38
3.2.1.5 Trojans, Vírus e Backdoors	38
3.2.1.6 “Instant Message” (IM) não criptografada	39
3.2.1.7 Confidencialidade	39
3.2.1.8 Autenticação e Autorização	39
3.2.2 **Ameaças Internas**	40
3.2.2.1 Interoperabilidade	40
3.2.2.2 O fator humano	40

3.2.3 **Mecanismos de Segurança** 40
3.2.3.1 Chave Privada (Private Key) 41
3.2.3.2 Chave Pública (Public Key) 41
3.2.4 **Futuro da Segurança P2P** 42
3.2.4.1 Confiabilidade de usuários 42
3.2.4.2 Biometria 42
3.2.4.3 Criptografia por chave quântica 43
4 **ASPECTOS DE MOBILIDADE EM REDES P2P** 44
4.1 INTRODUÇÃO 44
4.2 CARACTERÍSTICAS DE REDES P2P-MÓVEL 44
4.3 RESTRIÇÕES DAS REDES P2P-MÓVEL 45
4.4 APLICAÇÕES EM REDES P2P-MÓVEL 46
4.4.1 **MobileMule** 47
4.4.2 **PocketSkype** 48
5 **TRABALHOS RELACIONADOS** 49
5.1 SEGURANÇA 49
5.2 MOBILIDADE 51
6 **CONCLUSÃO** 53
GLOSSÁRIO 55
REFERÊNCIAS BIBLIOGRÁFICAS 56

1 **INTRODUÇÃO**

As redes P2P[1] (Peer-to-Peer) começaram a ser utilizadas a partir da década de 80, quando então analistas da indústria e profissionais da área começaram a acreditar que a sua utilização seria uma tendência irreversível, quase tanto como foi o começo do uso da internet. Foi quando novos projetos começaram a ser desenvolvidos, passando a oferecer mais opções para os usuários comuns, tais como Napster [21], SETI@home [22], Freenet [23], Gnutella [24], Jabber [25], etc. Usuários localizados em pontos isolados na internet passaram a conseguir compartilhar arquivos e formar comunidades na grande rede. Tentava-se eliminar com isso o conceito de clientes e servidores (pelo menos em sua essência básica), ocorrendo uma comunicação significativa entre pontos em cooperação.

1.1 MOTIVAÇÕES

Existem basicamente duas grandes motivações para o desenvolvimento de aplicações P2P [3]. A primeira refere-se a capacidade de processamento e armazenamento ociosa nos computadores conectados a Internet. As aplicações P2P podem fazer uso destes recursos ociosos para suportar um grande número de usuários acessando um mesmo sistema, sem a necessidade de nós centrais de processamento. Isto é possível pois estas aplicações possuem características como suporte a computação distribuída, redundância e tolerância a falhas.

Esta é a principal motivação para a utilização de redes P2P, pois o modelo cliente-servidor necessita de nós centrais com um grande poder de processamento, devido a crescente demanda exigida pelos novos sistemas e aplicações. As redes P2P não apresentam a necessidade de um alto investimento em máquinas centrais de coordenação.

---

[1] *Redes P2P - "Um tipo de rede de computadores onde cada estação possui capacidades e responsabilidades equivalentes, diferentemente da arquitetura cliente/servidor." (www.webopedia.com)*

A segunda motivação refere-se ao grande desejo de “anonimato” por parte dos usuários da Internet, que anseiam por descobrir novos métodos de compartilhamento de material protegido por direitos autorais (em sua grande maioria, arquivos de músicas) e para a livre expressão de suas idéias.

Outros dois fatores também explicam a motivação para o desenvolvimento das redes P2P. A sua natureza descentralizada e distribuída torna estas redes inerentemente robustos a certos tipos de problemas [4], fazendo com que sejam altamente indicadas para aplicações que necessitam de grande capacidade de armazenamento e processamento de longa duração. Além disso, o modelo P2P apresenta o benefício da escalabilidade para tratar de crescimentos incontroláveis no número de usuários e equipamentos conectados, capacidade de rede, aplicações e capacidade de processamento.

1.2 CONCEITO DE P2P

Apesar de haver diversas definições na literatura, todas elas convergem no seguinte conceito: redes P2P são redes virtuais que funcionam na Internet com o objetivo de compartilhar recursos e serviços computacionais entre os participantes, não existindo diferenciação entre os mesmos [4].

1.3 TRABALHOS RELACIONADOS

São contemplados também nesta pesquisa alguns trabalhos relacionados aos aspectos de segurança e mobilidade em redes P2P. Um dos principais trabalhos encontrados refere-se a utilização do modelo SPKI/SDSI (Simple Public Key Infrastructure / Simple Distributed Security Infrastructure), garantindo uma maior segurança para as aplicações P2P [18]. Outro trabalho referente a este aspecto aborda um modelo baseado nas tecnologias JXTA e

P2Psockets [19]. Quanto aos aspectos de mobilidade, será apresentado um trabalho sobre a tecnologia P2P Móvel [17].

1.4 OBJETIVOS

Recentemente aspectos relacionados à mobilidade e à segurança passaram a ser motivos de estudo neste tipo de redes. Com o advento das redes sem fio e com as questões cada vez mais presentes sobre aspectos de segurança, começou-se a notar a necessidade de se adequar estas questões às redes P2P.

O objetivo deste trabalho é apresentar os conceitos básicos relacionados aos sistemas P2P, assim como entender os principais problemas enfrentados, as tendências que o mercado apresenta e descrever alguns dos trabalhos recentes sobre o tema. São apresentados também aspectos de segurança e mobilidade dos sistemas P2P. Para isto serão conduzidas pesquisas em sites acadêmicos e corporativos, objetivando encontrar estudos de caso e tendências futuras para a utilização destes conceitos.

1.5 ORGANIZAÇÃO

Esta dissertação está estruturada em seis capítulos. O segundo capítulo apresenta os conceitos básicos necessários a um bom entendimento dos sistemas e redes peer-to-peer, como definições e características, redes overlay, modelos de arquitetura P2P, classificações existentes, aplicações P2P, projetos de sistemas P2P. O terceiro capítulo descreve as questões sobre segurança e o quarto apresenta os itens relacionados a mobilidade em redes P2P. O quinto capítulo apresenta alguns trabalhos relacionados. Finalmente, o sexto capítulo apresenta as conclusões finais e possíveis trabalhos futuros.

2 **CONCEITOS BÁSICOS**

2.1 INTRODUÇÃO

Embora o termo P2P provavelmente não seja conhecido por todas as pessoas, uma grande parte dos usuários da internet possivelmente já tenha utilizado alguns serviços oferecidos por esta tecnologia. É o caso do Napster, aplicação que foi utilizada por milhões de usuários da Internet. Praticamente não é mais usado, devido à forte pressão exercida pela indústria fonográfica mundial pelo combate à pirataria. O Napster foi considerado um projeto de impacto revolucionário, pois os usuários trocavam dados diretamente de seus discos rígidos de um sistema para outro. Máquinas de diferentes lugares do planeta se interconectando diretamente, trabalhando em conjunto para se tornarem supercomputadores virtuais, sistema de arquivos e mecanismos de pesquisa.

Além dos problemas de ordem legal, existem também as limitações técnicas. A principal delas é o grande consumo de largura de banda. A grande utilização por parte dos usuários começaram a saturar as redes de empresas e universidades. Restrições começaram a ser impostas a estes usuários por parte das corporações e dos provedores de acesso, com o objetivo de minimizar o tráfego gerado e adequar os usuários às normas legais existentes.

Apesar de ter como proposta principal o acesso irrestrito a todos os recursos da rede, de qualquer lugar e a qualquer hora, a Internet ainda está muito presa ao modelo cliente-servidor, no qual servidores centralizados executam tarefas para clientes distribuídos, como PCs, laptops e telefones celulares. Ou seja, a maior parte das máquinas participam da Web apenas acessando recursos providos pela minoria.

Segundo SADOK [4], a tecnologia P2P surgiu para mudar este conceito, pois não depende de uma organização central ou hierárquica. Por isso, os sistemas P2P devem possuir as seguintes características:

- nós podem estar localizados nas bordas da rede;
- nós com conectividade variável ou temporária;
- nós contendo endereços variáveis;
- capacidade de lidar com diferentes taxas de transmissão entre nós;
- nós com autonomia parcial ou total em relação a um servidor centralizado;
- assegurar que os nós possuam capacidades iguais de fornecer e consumir recursos de seus *peers*;
- a rede deve ser escalável;
- a capacidade dos nós se comunicarem diretamente uns com os outros.
- os nós são conectados de forma aleatória, não há restrição sobre o número de nós que participam da rede.
- a conexão de um nó à rede se estabelece através de outro nó que já pertença à rede.
- os nós podem se unir e sair da rede a qualquer momento sem prévio conhecimento dos demais membros.

Para que uma rede possa ser definida como peer-to-peer, ela precisa ter todas estas características, mesmo que algumas das funções de controle da rede estejam localizadas em um servidor central (o que representa um ponto de falha).

2.2 REDES P2P E REDES OVERLAY

Uma rede é considerada “overlay” quando é criada sobre uma rede existente. Ou seja, ela funciona como uma rede “virtual”. Um exemplo de rede overlay é a própria Internet, utilizando a infra-estrutura IP.

Uma rede overlay cria uma arquitetura com nível mais alto de abstração, de forma a solucionar vários problemas que, em geral, são difíceis de serem tratados ao nível dos roteadores da rede subjacente. No exemplo citado anteriormente, a Internet pratica o paradigma overlay quando usa o protocolo IP como solução de internetworking sobre tecnologias de redes diversas como ATM, Frame Relay, PSTN, LANs, etc. [4].

Desta forma, uma rede P2P pode ser considerada como sendo uma rede do tipo overlay, uma vez que é uma rede virtual formada pela interconexão dos *peers*, funcionando sobre a infra-estrutura de uma rede física.

2.3 CLASSIFICAÇÃO DOS MODELOS DE ARQUITETURA P2P

Existem cinco principais formas de classificar os modelos de arquitetura P2P [4]. Na primeira forma de categorização, são considerados dois modelos de rede P2P que são descritos a seguir.

- Descentralizado – não há a figura de um ponto central, isto é, cada nó tem o mesmo nível de importância. Neste modelo todos os nós são autônomos e responsáveis pela troca e gerenciamento dos recursos, podendo se comunicar de maneira direta ou através de vizinhos comuns (melhor escala de informações de controle, pior escala de tráfego de rede).

- Semi-centralizado – neste tipo de modelo há diferenças de relevância entre os nós. Em geral, existe um nó central responsável pelas informações de controle (e, possivelmente, para tráfego de dados) ou um conjunto de "super-nós" que assume tais funções (onde a queda de um super-nó afeta apenas os nós inferiores ligados a ele). Os nós inferiores podem ter maior ou menor nível de autonomia, mas são equivalentes entre si.

A segunda forma de categorizar os modelos de redes P2P, também muito utilizada, apresenta três tipos de arquitetura:

- busca centralizada – rede composta por um ponto central de busca (possivelmente espelhado para outros pontos, dando a impressão de serem vários deles) e por nós que consultam o ponto central para trocar informações diretamente entre os *peers*.

- busca por inundação – rede composta por nós totalmente independentes, onde normalmente a busca é limitada à vizinhança mais próxima do nó que iniciou o processo de busca (assim, a busca é escalável, mas não é completa).

- busca por tabela hash distribuída (*DHT – Distributed Hash Table*) – rede composta por nós com autonomia e que usam uma tabela hash para separar o espaço de busca entre eles.

A terceira classificação é bastante utilizada no meio acadêmico e apresenta três tipos de arquitetura:

- Centralizada - rede que mantém um índice central com informações atualizadas (similar à busca centralizada da classificação anterior). Sistemas de

compartilhamento de arquivos (Ex. Napster) e de troca de mensagens utilizam esta arquitetura.

- Descentralizada e Estruturada - rede que não possui um servidor centralizado de diretório de informações, mas que tem uma estruturação significativa entre os nós. A topologia da rede é controlada e os documentos e arquivos são posicionados em locais que posteriormente tornam fácil a sua localização. Esse tipo de arquitetura em geral utiliza busca baseada em DHT. Essa arquitetura é utilizada por vários sistemas, como por exemplo Chord, Pastry, Tapestry e CAN.

- Descentralizada e Não-Estruturada - rede que não possui servidor centralizado, nem controle preciso sobre a topologia e busca de documentos. Compreende os dois tipos (descentralizado e semi-centralizado) da primeira classificação e a busca por inundação da segunda. As redes Gnutella e KaZaA são dois exemplos de utilização desta arquitetura.

A quarta forma de classificação, segundo TOWSLEY [5], divide as redes P2P em três tipos.

- CIA (Centralized Indexing Architecture) – uma rede P2P segundo uma arquitetura CIA contêm um servidor central ou um cluster de servidores que é responsável por responder aos pedidos de busca e realizar todas as tarefas de manutenção da infra-estrutura. Um exemplo deste tipo de rede é o Napster.

- DIFA (Distributed Indexing with Flooding Architecture) – esta arquitetura, assim como as redes do tipo DIHA, é caracterizada pela completa descentralização de seu funcionamento. Os mecanismos de busca e manutenção da infra-estrutura

estão distribuídos pela rede. Neste tipo de sistema, cada nó é responsável por manter a listagem dos seus próprios arquivos, e responder quando receber uma busca por um arquivo (quando existir uma resposta válida para a busca em questão). Para isto, é utilizado o mecanismo de "flooding" ou inundação. A rede deste tipo mais conhecida e estudada é a rede **Gnutella**.

- DIHA (Distributed Indexing with Hashing Architecture) - esta arquitetura também possui uma característica totalmente descentralizada. A principal diferença entre as redes DIFA e DIHA está no mecanismo de busca. Nos sistemas com inundação, cada peer é responsável pelo espaço de índices relativo aos arquivos que ele próprio possui. Na arquitetura DIHA, ao contrário dos sistemas de inuncação, cada nó é responsável por um subconjunto do espaço total de índices. Quando o nó entra na rede, recebe um espaço do conjunto dos índices dos arquivos e, ao sair da rede, a mesma deverá designar estes índices para outro nó. As buscas não são difundidas na rede sem direção como no caso do “flooding”. Ao contrário, são direcionadas para o nó correto que é o responsável pelo respectivo índice dentro do espaço de índices. O protocolo mais conhecido deste modelo é o **Chord**.

A quinta proposta divide as redes P2P em dois tipos [6], conforme descrito a seguir.

- Pura - uma rede P2P é denominada “pura” quando possui uma arquitetura inteiramente distribuída e não necessita de um elemento central para o seu funcionamento. O Gnutella é o primeiro exemplo de uma grande rede P2P pura em funcionamento. Os modelos DIFA e DIHA relacionados anteriormente podem sem classificados como redes puras.

- Híbrida - a arquitetura do Napster não é inteiramente distribuída, conforme dito anteriormente. Isto explica-se porque ele depende sempre de um elemento central (servidor) para o seu funcionamento. Desta forma, pode-se classificar este tipo de rede como híbrida. Relacionando com a nomenclatura anterior, as redes do tipo CIA podem ser consideradas como híbridas.

2.4 DESCENTRALIZAÇÃO EM SISTEMAS P2P

Na prática, muitos aplicativos P2P utilizam abordagens híbridas em suas arquiteturas, devido a dificuldade em se desenvolver sistemas totalmente descentralizados [1]. Alguns exemplos de sistemas que são P2P no núcleo mas que possuem uma organização semicentralizada são o DNS, a Usenet, as mensagens instantâneas e o Napster.

A Usenet, sistema não mais utilizado, é um bom exemplo da evolução de um sistema descentralizado [1]. Concebido em 1979, a Usenet serviu como base para outros aplicativos P2P, como o Gnutella e a freenet. Fundamentalmente, é um sistema para cópia de arquivos entre computadores, sem a utilização de um controle central. O sistema era originalmente baseado em um recurso chamado protocolo UUCP (Unix-to-Unix Copy Protocol). A propagação da Usenet é simétrica, ou seja, os hosts compartilham o tráfego. Mas devido ao alto custo da alimentação das notícias (“Usenet News”), um backbone de hosts tornou-se responsável por carregar todo o tráfego e servir a um grande número de “nós-folha”, cujo papel principal é o de receber os artigos. É uma forma de “centralização suave”, tornando-se uma alternativa econômica para sistemas P2P com transmissão de dados de alto custo.

Assim como a Usenet, os aplicativos de mensagens instantâneas e o Napster também apresentam um perfil descentralizado, mas contam com um facilitador central para coordenar algumas operações. Os principais sistemas de mensagens instantâneas, por exemplo, possuem

algum tipo de servidor para facilitar a comunicação entre os nós. Este servidor mantém uma associação entre o nome do usuário e o seu endereço IP atual, armazenando em buffer as mensagens para o caso de o usuário estar desconectado e fazendo roteamento das mensagens para os usuários atrás dos firewalls.

2.5 APLICAÇÕES P2P

Nos sistemas P2P, segundo SADOK [4], todos os nós podem ser localizados, trazendo assim a conectividade para as bordas da rede e permitindo a comunicação e colaboração entre todos os equipamentos conectados (comunicação fim a fim). Desta forma, os sistemas P2P possibilitam um grande número de aplicações, como por exemplo o compartilhamento de arquivos, novas formas de distribuição e entrega de conteúdo, mensagens instantâneas, trabalho e lazer colaborativos, busca distribuída e compartilhamento de capacidade de armazenamento e processamento.

2.5.1 **Compartilhamento de Arquivos**

A troca e o armazenamento de conteúdo é uma das áreas onde a tecnologia P2P alcançou maior sucesso. Várias aplicações foram e têm sido usadas por usuários da Internet para burlar as limitações de largura de banda dos servidores, que em geral, impedem a transferência de arquivos grandes. Os sistemas de armazenamento distribuído baseados na tecnologia P2P utilizam as vantagens da infra-estrutura existente para oferecer as características descritas a seguir:

- *Áreas de armazenamento* – sistemas como Freenet (http://freenet.sourceforge.net) fornecem ao usuário uma área potencialmente ilimitada para o armazenamento de arquivos.

- *Alta disponibilidade do conteúdo armazenado* – para garantir alta disponibilidade dos arquivos armazenados, alguns sistemas adotam uma política de replicação múltipla do conteúdo, ou seja, um arquivo pode ser armazenado em mais de um nó na rede.

- *Anonimato* – alguns sistemas P2P como Publius [52] garantem matematicamente que os autores dos documentos publicados serão mantidos.

- *Gerenciamento* – a maioria dos sistemas P2P fornece mecanismos eficientes de localização e recuperação dos conteúdos armazenados na rede.

Segundo MILOJICIC [9], as principais questões técnicas relacionadas a sistemas de compartilhamento de arquivo são o consumo de largura de banda da rede, segurança e sua capacidade de pesquisa. São descritos a seguir os principais sistemas de compartilhamento de arquivos.

2.5.1.1 Napster

Este sistema representou uma grande inovação pois possibilitou a troca de arquivos entre vários usuários de forma direta entre a fonte e o destino. Contudo, os participantes não são capazes de descobrir a localização dos arquivos desejados de forma distribuída. Para esta tarefa, dependem de um servidor central.

Funciona da seguinte forma: o usuário deve se conectar ao sistema através de um servidor central e então fornecer a lista dos seus arquivos que estará compartilhando. Outro usuário conectado fará uma busca por arquivos que será respondida pelo servidor central. O programa cliente Napster, instalado no computador dos usuários, faz uma consulta ao servidor Napster para obter informações sobre o arquivo desejado. O servidor Napster responde se

existe o arquivo desejado e onde ele está localizado. Caso exista, uma conexão direta é estabelecida com o computador onde o arquivo está armazenado para que seja efetuado o download. Os arquivos são transferidos utilizando o protocolo http diretamente entre a fonte e a origem, sem intervenção do servidor.

Pode-se notar facilmente que esta arquitetura não é inteiramente do tipo P2P, uma vez que as buscas são respondidas de uma forma cliente/servidor tradicional (embora a transferência dos arquivos ocorra de forma distribuída). Mesmo não representando uma arquitetura inteiramente P2P, a arquitetura do Napter é uma bom exemplo a ser seguido em uma implementação real, uma vez que apresenta algumas vantagens.

Existe uma variedade de aplicações P2P semelhantes ao Napster no que se refere a funcionalidade e algumas das mais populares são: Dmusic (http://www.dmusic.com), Audiogalaxy (http://www.audiogalaxy.com), MyNapster (http://www.mynapster.com) e Wippit (www.wippit.com) .

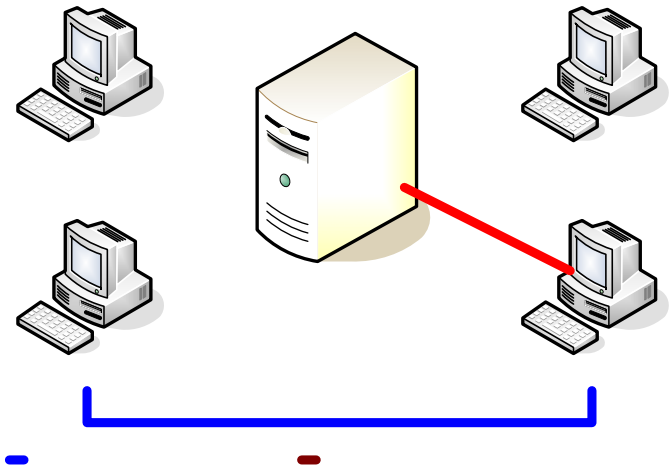

Figura 1 – Arquitetura do Napster

2.5.1.2 Gnutella

O Gnutella (http://www.gnutella.com) é considerado a primeira solução puramente P2P. Diferentemente do Napster, não existe um servidor central que armazena informações

sobre os arquivos que estão disponíveis na rede. Em vez disso, todas as máquinas da rede informam sobre os seus arquivos disponíveis usando um mecanismo de inundação e utilizam uma abordagem de busca distribuída para recuperá-los. Existem muitas aplicações cliente disponíveis para acessar a rede Gnutella, algumas das mais populares são: BearShare (http://www.bearshare.com), Gnucleus (http://www.gnucleus.com), LimeWire (http://www.limewire.com), WinMX (http://winmx.com) e XoloX (http://www.holox.com).

Segundo nomenclatura da especificação Gnutella, cada nó ou peer é chamado de servent. Conforme características das redes P2P, cada servent pode atuar como cliente ou servidor. Desta forma, eles possuem uma interface "servidor" para responder buscas dos pares e também possuem uma interface "cliente" para realizar suas próprias buscas. Como resultado, uma rede de servents Gnutella é altamente redundante, não tendo o serviço interrompido caso vários nós estejam desligados ou com apresentando problemas.

No site www.clip2.com [8] encontra-se uma descrição completa da versão 0.4 do protocolo Gnutella. Esta especificação do Gnutella define uma série de ***descriptors*** que são utilizados na comunicação entre os peers. Os ***descriptors*** são as mensagens trocadas entre os ***servents*** pelo protocolo Gnutella. Adicionalmente, algumas regras gerenciam a troca destas mensagens que, em conjunto, formam a especificação do protocolo. No quadro 1 encontra-se os ***descriptors*** e suas funções.

Quadro 1 – Quadro de Descriptors

Descriptor	Descrição
Ping	Utilizado para ativamente descobrir nós da rede. Quando um ***servent*** recebe um Ping, espera-se que o mesmo responda com um Pong.
Pong	Somente enviado em resposta ao Ping. Inclui o endereço de um ***servent*** e a quantidade de dados disponibilizada pelo mesmo
Query	Utilizado no mecanismo de busca distribuída na rede. O ***servent*** que recebe um Query deve responder com QueryHit se possuir o dado procurado na busca
QueryHit	A resposta para Query. Inclui informação para o *download* do arquivo Procurado
Push	Utilizado em um mecanismo para permitir que um nó atrás de um *firewall p*ossa contribuir com arquivos

Um ***servent*** se conecta a rede Gnutella estabelecendo uma conexão com outro peer que já esteja conectado a rede. O procedimento de aquisição do endereço de um host já conectado a rede Gnutella não faz parte da especificação do protocolo. Atualmente o método predominante é a utilização de arquivos ***cache*** com endereços pré-configurados. Após obter o endereço de outro ***servent*** conectado a rede, uma conexão TCP é estabelecida com o mesmo através do envio de uma mensagem CONNECT. Caso o receptor deseje se conectar, o mesmo deve responder com a mensagem OK. Qualquer resposta diferente indica que a conexão não será aceita. Um ***servent*** pode recusar uma conexão por uma série de motivos (não suporta a versão do protocolo solicitado, não possui capacidade para receber mais conexões, etc.).

Após a conexão a rede, o ***servent*** se comunica com outros servents através da troca de ***descriptors***, que são as mensagens trocadas na comunicação. Toda mensagem possui um cabeçalho que inclui, de forma resumida, uma identificação do tipo de ***descriptor*** que a mensagem representa, um identificador único da mensagem e um campo do tipo TTL que será utilizado para conter a inundação.

A figura 1 apresenta a diferença básica entre o funcionamento do Napster e do Gnutella, dois sistemas clássicos que impulsionaram o uso das redes P2P. Segundo Rocha (2003), o entendimento destes sistemas é o ponto de partida para o entendimento dos

conceitos P2P. O Napster possui um *cluster* de servidores para responder aos pedidos de busca, enquanto que o Gnutella realiza as buscas de forma distribuída.

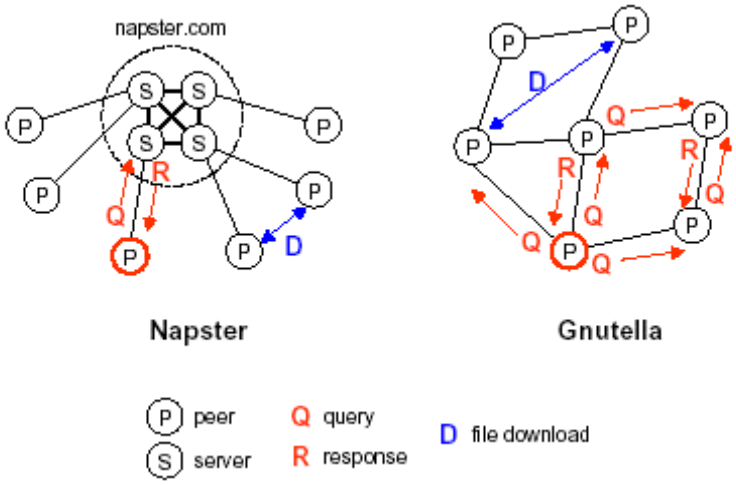

Figura 2 – Diferença entre Napster e Gnutella

2.5.1.3 Freenet

O Freenet é um software livre que permite que seus usuários publiquem e obtenham informações na Internet. Para tal, a rede é completamente descentralizada e os usuários são mantidos no anonimato. As comunicações dos usuários são sempre cifradas, tornando extremamente difícil determinar quem está solicitando a informação e qual é o seu conteúdo.

Segundo ROCHA [2], os usuários contribuem com a rede fornecendo largura de banda e espaço para armazenamento dos dados. O Freenet não deixa o usuário controlar o que é armazenado no espaço de dados. Ao invés disso, os arquivos são mantidos ou excluídos de acordo com a frequência de acessos (arquivos acessados com menor freqüência são descartados), ajudando a manter o conteúdo do espaço de dados sempre atualizado.

2.5.1.4 KaZaA

O KaZaA (http://www.kazaa.com), sistema de compartilhamento de arquivos mais utilizado na Internet, utiliza o conceito de "supernós" para melhorar o desempenho da rede. Um supernó é uma máquina que participa da rede (nó) e que possui um alto poder computacional e rápidas conexões com a Internet. Os supernós mantêm uma lista contendo os arquivos disponibilizados por outros usuários e o local onde eles estão armazenados. Quando uma busca é executada, a aplicação KaZaA procura primeiramente no supernó mais próximo do usuário que iniciou a consulta, retornando um conjunto de respostas para o usuário e encaminhando a consulta para outros supernós. Uma vez localizado o usuário que possui o arquivo, uma conexão é estabelecida diretamente entre os peers para que seja efetuado o download.

2.5.1.5 Outras Aplicações

Outras aplicações P2P de compartilhamento de arquivos são: AudioGnome (www.audiognome.com), Jungle Monkey (www.junglemonkey.net), Badblue (www.badblue.com), Napigator (www.napigator.com), eDonkey (www.edonkey.com), Project Elf (www.projectelf.com), eMule (www.emule-project.net), Shareaza (www.shareaza.com), Filetopia (www.filetopia.org), Snarfzilla (www.snarfzilla.sourceforge.net), Frost (www.jtcfrost.sourceforge.net), Spinfrenzy (www.spinfrenzy.com), Grokster (www.grokster.com), Splooge (www.splooge.com), Imesh (www.imesh.com).

2.5.2 **Troca de Mensagens**

As trocas de mensagens instantâneas (IM – Instant Messaging) se tornaram uma das aplicações mais populares da Internet. Diferentemente do correio eletrônico, em que uma mensagem é armazenada em uma caixa postal e posteriormente entregue ao usuário que verificou a caixa postal no seu servidor, os sistemas IM fornecem entrega imediata ao usuário. Se o usuário não está disponível, a mensagem pode ser armazenada até que o mesmo se torne "on-line", ou ela pode ser simplesmente descartada. Para evitar esta incerteza na entrega, os sistemas IM fornecem uma lista de contatos com um mecanismo capaz de identificar um usuário e determinar o seu estado, por exemplo, "online", "offline" ou ocupado.

Algumas das soluções de IM são apresentadas a seguir.

2.5.2.1 MSN Messenger

O MSN Messenger da Microsoft (http://msn.com) é a mais popular ferramenta de IM disponível no momento. Permite comunicação em tempo real (fornece sincronização de vídeo e voz).

2.5.2.2 Yahoo! Messenger

Uma característica interessante do Yahoo! Messenger (http://messenger.yahoo.com) é a sua boa integração com os serviços e conteúdos do site Yahoo!. Além disso, o usuário pode receber e enviar mensagens através do seu telefone celular, ser alertado instantaneamente quando há novas mensagens em seu Yahoo! Mail ou quando está na hora de um de seus compromissos na Yahoo! Agenda.

2.5.2.3 Outras Aplicações IM

Outras aplicações P2P para troca de mensagens são: ICQ (http://web.icq.com), JabberIM – (http://www.jabber.com), Messaging Architects – (http://www.gwtools.com), Omnipod – (http://www.omnipod.com), Sametime – (http://www.lotus.com/products/lotussametime.nsf/wdocs/homepage), Trillian Messenger – (http://www.trilian.cc), Vayusphere – (http://www.vayusphere.com).

2.5.3 **Outros Projetos P2P**

2.5.3.1 SETI@home

A origem do nome SETI surgiu de um projeto conduzido por dois amigos (David Anderson e David Gedye) [1]. O seu propósito básico era a utilização do potencial computacional dos PC's domésticos para procurar por sinais de rádio emitidos por civilizações extraterrestres (SETI – Search for Extraterrestrial Inteligence).

Juntamente com o Napster, o SETI@home (http://setiathome.ssl.berkeley.edu), foi um dos primeiros sistemas P2P a serem criados. Segundo ROCHA [2], ele possui um poder computacional de aproximadamente 25 TFlops/s (trilhões de operações de ponto flutuante por segundo), coletado de mais de três milhões de computadores conectados à Internet.

De modo geral, o funcionamento do SETI@home é composto pelos passos descritos a seguir. O problema computacional a ser resolvido é dividido em tarefas pequenas e independentes [2]. Um servidor central é responsável pela divisão das tarefas entre os computadores registrados na Internet. Em cada um desses computadores é instalado um software cliente que executa alguma computação requisitada pelo servidor. O processamento é realizado toda vez que o computador entra em período de inatividade. Desta forma, o

processamento de cada tarefa é feito em um computador individual e os resultados são coletados pelo servidor central, que distribui novas tarefas para os clientes.

2.5.3.2 Jabber

Uma das principais funcionalidades utilizadas na Internet é a conversação, seja ela entre pessoas, entre aplicações ou mesmo entre pessoas e aplicações. Visando unificar as conversações que se propagam pela Internet e também capacitar aplicações e serviços a executarem sob uma plataforma comum [1], uma comunidade de desenvolvedores em todo o mundo desenvolveu um conjunto de tecnologias conhecidas como Jabber (http://www.jabber.org/).

Inicialmente, o Jabber foi desenvolvido para a comunicação entre pares (seja entre pessoas ou entre aplicações) e para conversações em tempo real além de conversações assíncronas/offline [1]. O Jabber foi desenvolvido de forma totalmente distribuída, ao contrário dos serviços de *Instant Messaging*. A motivação foi o desejo de se criar uma plataforma totalmente aberta e distribuída para o envio de mensagens, oferecendo assim uma alternativa para os usuários que não quisessem utilizar os serviços comerciais centralizados.

As principais idéias do Jabber são descritas a seguir.

- Disponibilizar os recursos necessários para conversações entre pessoas e aplicações.
- Criar um ambiente "aberto", onde o usuário possa escolher o software para o gerenciamento das conversações (ao contrário de software comerciais de *IM*).
- Permitir e acelerar o desenvolvimento de aplicações pares construídas sobre este ambiente aberto, facilitando assim as conversações e o acesso a dados dinâmicos de diferentes serviços.

2.6 PLATAFORMAS DE DESENVOLVIMENTO P2P

Muitas aplicações P2P atuais não utilizam nenhum framework padrão para desenvolver suas aplicações. Entretanto, já existem plataformas de desenvolvimento que são utilizadas para alavancar a construção de novas soluções P2P, como JXTA, .Net e Groove.

2.6.1 **JXTA**

Inicialmente a tecnologia P2P foi utilizada em aplicações de função única, como por exemplo para comunicação instantânea (IM – Instant Messaging). Levando o conceito de P2P mais adiante, a Sun Microsystems concebeu a idéia do Projeto JXTA como um meio de integrar a tecnologia P2P ao núcleo da arquitetura de rede [10].

O Projeto JXTA é um conjunto de protocolos P2P simples e abertos que habilitam os dispositivos na rede a se comunicarem, colaborarem e compartilharem recursos [2]. Os peers JXTA criam uma rede virtual ***ad hoc*** no topo de redes existentes, mascarando a complexidade existente nas camadas de baixo. Na rede virtual JXTA, os ***peers*** podem interagir entre si, independente de sua localização, tipo de serviço ou ambiente operacional (mesmo quando alguns ***peers*** e recursos estão posicionados atrás de firewalls ou estão em diferentes tecnologias de transporte de rede). Assim, o acesso aos recursos da rede não é limitado por incompatibilidades de plataforma ou restrições da arquitetura cliente/servidor.

Segundo ROCHA [2], a tecnologia do projeto JXTA adota como objetivos: interoperabilidade (entre diferentes sistemas e comunidades P2P), independência de plataforma (diversas linguagens, sistemas e redes), generalidade (qualquer tipo de dispositivo digital) e segurança. A tecnologia JXTA funciona em qualquer dispositivo, incluindo aparelhos celulares, PDAs, sensores eletrônicos, estações de trabalho e servidores. A

tecnologia é baseada em tecnologias aprovadas e padronizadas como HTTP, TCP/IP e XML, e não é dependente de nenhuma linguagem de programação particular, sistema de rede, ou plataforma de sistema, podendo inclusive trabalhar com uma combinação de alguns deles.

A plataforma JXTA pode ser descrita simplesmente como uma tecnologia que permite a comunicação entre peers. Cada peer é associado a um identificador único, um "peer ID", e pertence a um ou mais "peergroups". Os peers cooperam e têm funções similares, sob um conjunto unificado de capacidades e restrições. A plataforma JXTA provê alguns protocolos para as funções básicas: criar e encontrar grupos, entrar e sair de grupos, monitorar os grupos, conversar com outros grupos e peers, compartilhar conteúdo e serviços, etc. Estas funções são realizadas através da publicação e troca de anúncios XML e mensagens entre os peers.

Conceitualmente, cada peer na plataforma JXTA possui três camadas: o núcleo, a camada de serviços e a camada de aplicação.

O núcleo é responsável por gerenciar o protocolo JXTA, encapsulando o conhecimento de todas as operações P2P básicas. Ou seja, ele contém as funcionalidades e a infra-estrutura suficientes para o desenvolvimento de qualquer aplicação P2P. A camada de serviço, por sua vez, armazena as funcionalidades comuns que mais de um programa P2P poderia utilizar. Ela provê funcionalidades similares a de uma biblioteca, que pode ser controlada pelas aplicações JXTA através de lógica na camada de aplicação. Finalmente, a camada de aplicação é aquela onde a aplicação P2P realmente reside. Ela pode permitir que o usuário controle diferentes serviços, ou pode ser onde a lógica de uma aplicação autônoma opera. Por exemplo, um simples programa de bate-papo pode ser construído nessa camada, fazendo uso tanto do serviço quanto do núcleo para permitir que os peers troquem mensagens.

A plataforma JXTA provê ainda um conjunto de blocos que permitem uma sólida base para aplicações computacionais distribuídas e dão suporte a funções comuns requeridas por qualquer sistema P2P. Utilizando esses recursos, os desenvolvedores podem elaborar suas aplicações P2P mais facilmente. Existem APIs para outras linguagens, como por exemplo Java e C++. Os protocolos JXTA estão especificados em alto-nível e, portanto, podem ser implementados teoricamente em qualquer linguagem.

A arquitetura JXTA já sofreu modificações significativas com o objetivo de possibilitar a criação de redes P2P de melhor desempenho, maior escalabilidade e facilidade de manutenção. Maiores informações sobre a plataforma podem ser encontradas no site do projeto(http://www.jxta.org).

2.6.2 **.NET**

A plataforma .Net disponibiliza um conjunto de alternativas que podem ser utilizadas para construir aplicações P2P. Entretanto, segundo ROCHA [2], é importante conhecer como as funcionalidades podem ser utilizadas, para tornar mais fácil a escolha do modelo mais adequado a cada aplicação. A plataforma .NET disponibiliza quatro modelos de aplicação para P2P [11], que são descritos a seguir:

- Serviços Web (Web Services): provê mecanismos para fazer registro, descoberta e recuperação (download) para aplicações P2P
- Formulários (Windows Forms): essa é a solução fornecida pela plataforma .NET para facilitar a construção de interfaces gráficas sofisticadas

- Processo de Serviços (Service Process): este tipo de solução é muito útil para construir soluções que requerem processos distribuídos, como o projeto SETI@home, pois permite compartilhar e localizar os serviços disponíveis.

- Formulários Web (Web Forms): permite que as aplicações P2P realizem o download de conteúdo HTML de forma mais fácil.

2.6.3 **Groove Development Kit (GDK)**

O GDK é uma plataforma para desenvolvimento de aplicações P2P que pode ser utilizada gratuitamente. Entretanto, estas aplicações só podem ser utilizadas mediante a obtenção de uma licença. Esta ferramenta foi desenvolvida utilizando o *Microsof Component Object Model (COM),* o que torna os programas dependentes da plataforma de desenvolvimento Microsoft.

Segundo ROCHA [2], o GDK utiliza uma abordagem híbrida, o que permite o emprego de solução centralizada ou descentralizada. Além disso, disponibiliza alguns serviços, como: armazenamento de mensagens enviadas para clientes off-line; serviços de interface gráfica; gerenciamento de dados (permitindo manipular facilmente dados sincronizados); compartilhamento de espaço (possibilitando acessar ferramentas em tempo de execução); serviço de identificação (permitindo localizar usuários *on-line*); ferramentas de publicação (o que possibilita disponibilizar, criar e testar as ferramentas desenvolvidas).

3 **ASPECTOS DE SEGURANÇA EM REDES P2P**

3.1 INTRODUÇÃO

A segurança é uma questão fundamental para qualquer sistema de computação. A importância da segurança em sistemas P2P pode ser explicada através de vários fatores, como por exemplo as fraudes nas grandes corporações e perdas de receitas devidos a ataques a redes internas. O Napster foi o primeiro sistema a ser motivo de atenção quanto a questões de segurança [13], mas desde então outras aplicações P2P têm causado dores de cabeça nas grandes corporações mundiais, devido a ataques "maliciosos" na utilização de sistemas P2P.

Para tentar reduzir a ocorrência destes ataques, existe uma preocupação cada vez maior com processos internos, como os controle de conexão, de acesso, de operação, atualização de software anti-vírus e proteção dos dados armazenados.

3.2 PROBLEMAS

Os principais problemas de segurança das redes P2P [13] são descritos a seguir.

3.2.1 **Ameaças Externas**

As redes P2P possuem vulnerabilidades que podem dar origens a vários ataques. A maioria deles se manifestam através de ameaças já conhecidas, como worms e vírus.

Além disto, as redes P2P sofrem outros tipos de riscos, como "downloads" não autorizados e utilização de material que viole as leis de direitos autorais. Aplicações como Napster e KaZaa eram muito populares entre os usuários de Internet. Por isso, não eram raros os casos de utilização de redes corporativas de alta velocidade para este tipo de "download". Esta situação gerava numerosos problemas para a empresa, pois tornava a rede vulnerável a

ataques e a arquivos infectados por vírus, além de representar uma alta utilização da banda para fins não-corporativos. Recentemente a utilização de ferramentas de trabalho para fins pessoais tornou-se crime com jurisprudência no Brasil, após um caso de demissão de funcionário de uma grande instituição financeira que utilizou o correio eletrônico para troca de mensagens de cunho pessoal.

As ameaças externas mais conhecidas [13] são descritas a seguir.

3.2.1.1 Roubo

Empresas podem perder milhões em propriedades roubadas, como o código fonte de seus produtos. Ferramentas de "Warpping" podem disfarçar um arquivo ".zip" contendo um código fonte de uma empresa, em um arquivo de música MP3. Como resultado, uma terceira pessoa pode acessar este arquivo através de uma rede P2P (através por exemplo de um acesso via KaZaa) e vendê-lo para uma empresa concorrente.

3.2.1.2 Obstrução de largura de banda e compartilhamento de arquivo

O maior problema com o compartilhamento de arquivos é o enorme tráfego gerado, obstruindo a rede das instituições, afetando a comunicação dos usuários internos da rede assim como seus clientes, fornecedores e usuários de comércio eletrônico. Consequentemente, resultaria em perdas de capital para a empresa.

3.2.1.3 Bugs

Falhas (mais conhecidas como "bugs") nas aplicações P2P para compartilhamento de arquivos. Podem expôr a rede a inúmeros riscos.

3.2.1.4 Quebra de criptografia

Processamento distribuído é uma outra aplicação P2P muito em evidência ultimamente. Possui como objetivo interligar vários computadores, resultando em uma enorme capacidade computacional para solucionar problemas mais complexos. Distributed.Net é um exemplo deste tipo de aplicação. Em 1999, em conjunto com o Eletronic Frontier Fondation (www.eff.org), o Distributed.Net lançou um ataque de força bruta no algoritmo de criptografia de 56 bits DES. Juntos, quebraram o DES em menos de 24 horas (somente o Distributed.Net tinha capacidade de testar 245 bilhões de chaves por segundo). Naquele tempo o DES era o algoritmo de criptografia mais forte que o governo dos Estados Unidos permitia exportar.

3.2.1.5 Trojans, Vírus e Backdoors

Um usuário de um sistema P2P pode instalar, sem perceber, um arquivo contaminado em sua estação, causando sérios danos aos demais computadores da rede. Por exemplo, um programa de compartilhamento de arquivos poderia incluir uma "backdoor", permitindo o acesso de outros usuários de computadores. Um usuário com conhecimento e com intenções maliciosas poderia causar sérios danos ou obter informações sigilosas.

Além disso, aplicativos P2P costumas burlar arquiteturas de segurança do mesmo modo que os Trojans. A aplicação P2P é instalada em "dispositivos confiáveis" que permitem a comunicação através do Firewall corporativo com outros usuários P2P (usuários externos). Uma vez estabelecida a comunicação, o usuário externo pode ter acesso remoto ao dispositivo confiável e, por exemplo, roubar dados confidenciais da corporação, lançar um ataque de "Denial of Service" ou simplesmente garantir o acesso aos recursos da rede.

3.2.1.6 “Instant Message” (IM) não criptografada

Os aplicativos de “Instant Message” (IM), como, por exemplo, o MSN Messenger, são uma ameaça a confiabilidade das informações de uma companhia. Um infrator pode ler todas as mensagens que são enviadas e recebidas por aplicativos IM através da rede ou da internet utilizando um programa de monitoração de rede (como por exemplo, o Ethereal)

Nas aplicações de IM têm sido incorporadas novas capacidades como, por exemplo, mensagens de voz e compartilhamento de arquivos. Adicionando a funcionalidade de compartilhamento de arquivo aos aplicativos de IM, serão também adicionados todos os riscos que este tipo de aplicação apresenta, conforme apresentado no item 3.2.1.2.

3.2.1.7 Confidencialidade

O KaZaa e o Gnutella permitem que os usuários tenham acesso direto aos arquivos armazenados nos discos rígidos de outros clientes. Sendo assim, é possível a um “hacker” descobrir qual o sistema operacional utilizado em um computador, bem como acessar pastas ou arquivos de sistema.

3.2.1.8 Autenticação e Autorização

Uma outra questão de segurança muito importante trata sobre a autenticação e autorização entre usuários de sistemas P2P. Um usuário precisa saber quando um outro está solicitando, por exemplo, a transferência de um arquivo de seu computador, bem como conseguir identificá-lo. Somente após estes passos ele deve autorizar a transferência da informação. Estes passos servirão para evitar que usuários não autorizados consigam se conectar sem autorização prévia e, com isso, transferir informações sem a sua permissão, acessar dados confidenciais ou mesmo transferir vírus ou arquivos maliciosos.

3.2.2 **Ameaças Internas**

Existem também as ameaças internas que, não menos importantes que as externas, são descritas a seguir.

3.2.2.1 Interoperabilidade

É uma das principais questões relacionadas a segurança em redes P2P. A introdução de diferentes plataformas, sistemas e aplicações em uma mesma infra-estrutura resulta em uma série de questões a respeito de segurança associadas a interoperabilidade. Quanto maiores forem as diferenças dentro de uma mesma infra-estrutura, maiores serão os problemas de segurança existentes.

3.2.2.2 O fator humano

Sempre existirão usuários mal intencionados, dispostos a obterem acesso clandestino às redes corporativas. Independente do protocolo de segurança implementado, é apenas uma questão de tempo para que estes usuários encontrem uma maneira de burlar esses protocolos. É uma "guerra" sem fim, ou seja, os analistas de segurança tentando sempre se manter a frente dos "hackers", tentando prever futuras brechas no sistema e, desta forma, desenvolvendo novos mecanismos de segurança. Por outro lado, os "hackers" estarão sempre tentando sempre encontrar maneiras para burlar os mecanismos desenvolvidos.

3.2.3 **Mecanismos de Segurança**

A grande maioria dos sistemas de segurança são baseados em criptografia utilizando tanto chave simétrica/privada quanto chave assimétrica/publica, ou mesmo uma combinação

das duas. Esta seção apresenta os aspectos básicos das técnicas utilizadas pelas chaves públicas e privadas.

3.2.3.1 Chave Privada (Private Key)

Segundo o Grupo de Redes de Computadores da UNESP [15], encriptação por chave privada é o metodo que utiliza uma mesma chave para encriptar e desencriptar a mensagem. Esta chave pode ser uma palavra, uma frase ou uma sequência aleatória de números. O tamanho da chave é medido em bits e, via de regra, quanto maior a chave, mais seguro será o documento encriptado. A encriptação por chave privada funciona muito bem quando o usuário que encripta é o mesmo que desencripta o arquivo (por exemplo, para proteger arquivos que ficam armazenados no próprio disco rígido). Mas quando se trata de uma mensagem que vai ser transmitida, essa técnica apresenta problemas. O receptor e o transmissor precisam antes combinar uma senha, e usar algum meio seguro para transmitir esta informação (isso só ocorre quando se cria apenas uma chave). Um meio realmente seguro de transmissão de dados é muito caro e difícil de obter; e, se ele existe, então a própria mensagem poderia ser transmitida por ele.

3.2.3.2 Chave Pública (Public Key)

Encriptação por chave pública é o método que permite a transmissão de uma mensagem totalmente segura através de um canal inseguro [15]. O receptor da mensagem cria duas chaves que são relacionadas entre si, uma pública e uma privada. A chave pública pode e deve ser distribuída livremente. Quem envia a mensagem tem que utilizar a chave pública do receptor para encriptá-la. Uma vez encriptada, esta mensagem só pode ser decriptada pela chave do receptor.

3.2.4 **Futuro da Segurança P2P**

As redes P2P têm recebido cada vez mais atenção ao longo da sua existência. Cada vez mais as pessoas compartilham seus recursos e os sistemas tendem a ser distribuídos. Assim, torna-se cada vez mais importante a segurança das informações, uma vez que a indústria de fraudes também apresenta um rápido processo de evolução.

Muitas propostas para a segurança em ambientes P2P já estão em andamento [13]. Este item apresenta algumas delas.

3.2.4.1 Confiabilidade de usuários

O nível de confiabilidade associada aos usuários dentro de uma comunidade P2P é um item muito importante dentro dos aspectos de segurança de uma rede P2P. Todos os usuários devem possuir uma única assinatura digital (como por exemplo um IP), mas associada aos usuários e não às máquinas. Junto a esta assinatura deverá existir um nível de confiança, variando de acordo com uma escala. Dependendo do comportamento do usuário o seu grau de confiança deve aumentar ou diminuir.

3.2.4.2 Biometria

A biometria envolve o uso de uma característica pessoal para autenticar o usuário, como por exemplo, uma imagem facial da pessoa, uma assinatura, uma impressão digital ou um padrão de retina. A vantagem da característica biométrica é que os usuários não precisam lembrar de nenhuma senha ou armazenar nenhuma chave, que são os maiores pontos de vulnerabilidade em um sistema de autenticação convencional. Porém, nos últimos tempos têm-se cogitado em uma integração desta tecnologia com um sistema de autenticação maior,

talvez uma combinação com um certificado criptográfico. Desta forma, poderia-se ter uma solução mais robusta e menos vulnerável, ao invés de ter um ponto singular de defesa.

3.2.4.3 Criptografia por chave quântica

O desenvolvimento da técnica reunindo o conceito de criptografia e a teoria quântica é mais antigo do que se imagina, sendo anterior à descoberta da criptografia de Chave Pública [16]. Em [26], Stephen.Wiesner explica como a teoria quântica poder ser usada para unir duas mensagens em uma única transmissão quântica na qual o receptor poderia decodificar cada uma das mensagens porém nunca as duas simultaneamente devido à impossibilidade de violar uma lei da natureza (o Princípio de Incerteza de Heisenberg).

Utilizando-se fótons, a Criptografia Quântica permite que duas pessoas escolham uma chave secreta que não pode ser quebrada por qualquer algoritmo, em virtude de não ser gerada matematicamente, mesmo se utilizando um canal público e inseguro. É interessante notar que os métodos criptográficos passam a ter uma referência na Física, e não mais somente na Matemática.

A Criptografia Quântica se destaca em relação aos outros métodos criptográficos pois não necessita do segredo prévio, permite a detecção de leitores intrusos e é incondicionalmente segura, mesmo que o intruso tenha poder computacional ilimitado. Por apresentar um elevado custo de implantação, ainda não é um padrão adotado de segurança nas comunicações.

4 **ASPECTOS DE MOBILIDADE EM REDES P2P**

4.1 INTRODUÇÃO

A utilização de dispositivos móveis apresenta um alto crescimento atualmente, fazendo com que exista uma grande variedade de aparelhos utilizando tecnologia para a comunicação sem fio, como por exemplo Wi-Fi, Wi-Max, Bluetooth e GPRS [17]. Desta forma, aplicações P2P já estão sendo desenvolvidas para atender a esta tendência, como o "PocketSkype" (transmissão de voz sobre protocolo IP através de um pocket PC) e "MobileMule" (compartilhamento de arquivos através do uso de celulares).

Com isso, novos protocolos estão sendo criados para atender a estes *peers* móveis, assim como alterações em protocolos já existentes. Um exemplo destas modificações foi realizado pelo grupo GT-P2P (grupo de trabalho em computação colaborativa), que desenvolveu uma infra-estrutura denominada X-Peer [17], que utiliza protocolos no formato binário ao invés dos protocolos definidos em XML. O motivo é a redução do tempo de processamento, requisito fundamental para a utilização de aplicativos P2P em aparelhos móveis.

4.2 CARACTERÍSTICAS DE REDES P2P-MÓVEL

Uma rede P2P-Móvel permite a existência e participação de *peers* móveis, que podem ser aparelhos móveis ou aparelhos fixos. As aplicações que utilizam o conceito de P2P e que são executadas a partir de um dispositivo móvel são denominadas aplicações P2P-Móvel.

Esse peers possuem como característica um novo tipo de informação, a sua localização geográfica, que ser bastante útil dentro de uma comunidade P2P, dependendo dos objetivos de seus integrantes.

4.3 RESTRIÇÕES DAS REDES P2P-MÓVEL

O crescimento da utilização de dispositivos móveis (como por exemplo *handhelds*) trouxe novos desafios para a construção de aplicações P2P-Móveis [17]. Desta forma, existe a necessidade de uma compreensão correta de todos os requisitos e limitações que este ambiente oferece ao desenvolvimento destas aplicações.

Uma das questões a serem consideradas diz respeito às restrições impostas pelas redes P2P como, por exemplo, a utilização de equipamentos que possuam NAT (*Network Address Translation*) configurado ou aqueles que funcionem atrás de uma rede protegida por um *firewall*, restringindo a a alcançabilidade dos computadores [17]. Já existem técnicas que solucionam este tipo de problema, mas que, por outro lado, prejudicam o tempo de resposta. E tempo de resposta é um requisito fundamental em uma rede P2P-Móvel.

Um outro aspecto importante para o desenvolvimento de aplicações P2P-Móvel, é a interoperabilidade entre os novos protocolos e os já existentes. Sendo assim, devem ser consideradas as características dos principais protocolos como JXTA, JXME, Jabber, SIP, etc.

Existem também as restrições impostas pelos próprios dispositivos móveis que, quando comparados aos computadores utilizados em redes P2P (desktops), apresentam características que podem dificultar ou mesmo impossibilitar o seu uso neste tipo de rede. As principais são a baixa quantidade de memória, processamento, espaço para armazenamento e pouco tempo de vida das baterias (considerando-se logicamente a sua utilização sem conexão

direta com a energia elétrica). Entretanto, a constante evolução tecnológica que assola o mundo reduz estas limitações, porém muitas vezes a custos consideráveis.

Um outro tipo de limitação são as tecnologias de acesso (como por exemplo, 802.11 e 802.16). Basicamente o que diferencia estas tecnologias entre si são fatores como largura de banda, capacidade das mesmas de obter qualidade de serviço (QoS), disponibilidade da taxa de transferência e mecanismos de transporte [17]. E uma das principais limitações impostas refere-se justamente a uma largura de banda relativamente baixa. Como a performance é requisito fundamental em uma rede P2P-Móvel, tornam-se fundamentais algumas providências, como por exemplo a redução do overhead de sinalização.

Uma maneira para otimizar a comunicação entre peers móveis seria utilizar estratégias como caching [17], com o objetivo de reduzir a banda e o tráfego de sinalização. Entretanto, esta solução ainda não é utilizada em redes P2P-Móvel.

O aspecto econômico também deve ser levado em consideração nas redes P2P-Móvel. Os custos para o tráfego de dados em uma rede celular, por exemplo, ainda são muito caros, inviabilizando a utilização contínua desta tecnologia. Para que este tipo de serviço possa ser realmente utilizado, as operadoras precisam, além de reduzir os preços atuais, oferecer algum tipo de pacote de serviços P2P para estimular o seu uso. Aspectos como *copyright* e regulamentação também devem ser levados em consideração.

4.4 APLICAÇÕES EM REDES P2P-MÓVEL

Esta seção apresenta algumas das principais aplicações P2P-Móvel. São elas: MobileMule e PocketSkype.

4.4.1 **MobileMule**

O MobileMule foi originado do eMule, um aplicativo utilizado para o compartilhamento de arquivos através de uma rede P2P. Assim como vários outros aplicativos o eMule também funciona como um cliente P2P, possibilitando que o usuário esteja conectado a vários outros usuários simultaneamente, com o objetivo de compartilhamento de arquivos e recursos.

O grande crescimento da utilização de celulares com tecnologias que permitem o uso de redes sem fio (por exemplo, Bluetooth) motivou a criação do MobileMule [17], permitindo que o usuário controle remotamente uma máquina com cliente eMule sendo executado. Ou seja, qualquer dispositivo móvel poderia obter informações de máquinas que estejam participando de uma rede P2P, além de, por exemplo, iniciar a transferência de arquivos e compartilhamento de recursos. É interessante notar que o o celular que executa o MobileMule não é um cliente P2P, e sim apenas o dispositivo que o controle remotamente.

O funcionamento desta aplicação é descrita a seguir. O dispositivo com MobileMule (cliente) conecta-se ao equipamento eMule (servidor) através da porta 80 [17]. O MobileMule permite que o usuário realize diversas funções remotamente, como iniciar uma busca, realizar *download* de arquivos (para o cliente P2P, com eMule), checar status de arquivos e até mesmo visualizar o primeira quadro de um arquivo de vídeo. Pode-se ainda utilizar o MobileMule para desligar e ligar o computador remotamente.

Segundo OLIVEIRA [17], existe uma proposta atualmente de modificação da rede eDonkey para permitir que estes equipamentos móveis funcionem como um cliente P2P, participando efetivamente do compartilhamento de arquivos e recursos.

4.4.2 **PocketSkype**

O objetivo do Skype é fornecer serviço de telefonia na internet através do protocolo VoIP (Voice over Internet Protocol), permitindo assim que os usuários estabeleçam conversações de voz sem a utilização das operadoras telefônicas tradicionais.

Todas as máquinas que possuam o Skype sendo executado funcionam como um peer dentro de uma rede P2P, na qual o único elemento central é o servidor de autenticação (login) dos usuários [17]. Todos estas estações participantes têm a capacidade de enviar e receber simultaneamente stream de áudio em tempo real

Recentemente, foi lançado o primeiro produto que utiliza VoIP através de dispositivo móvel, chamado de PocketSkype. Foi desenvolvido para ser utilizado em PocketPCs (através de WLAN), mas já está desenvolvida uma versão para Bluetooth [17].

Segundo OLIVEIRA [17], é necessária uma conexão rápida para a utilização do PocketSkype. Sua performance foi considerada razoável quando utilizada em conexões ADSL de 256 Kbps (através de Wi-Fi ou Ethernet), mas extremamente ruim quando utilizada via USB ou Bluetooth.

5 **TRABALHOS RELACIONADOS**

5.1 SEGURANÇA

Existem vários trabalhos sendo conduzidos atualmente relacionados a segurança em redes P2P. Uma das atuais propostas sobre é encontrada em [18]. Apresenta um trabalho para prover uma maior segurança para aplicações que utilizam redes P2P, através do uso do modelo SPKI/SDSI (Simple Public Key Infrastructure / Simple Distributed Security Infrastructure), garantindo assim uma maior segurança para estas aplicações. Esta solução, além de garantir conceitos importantes para a segurança em redes P2P, como autenticidade, integridade, confidencialidade e um adequado controle de acesso, garante também propriedades como anonimato e reputação, igualmente necessárias neste tipo de rede.

Uma outra importante abordagem sobre segurança em redes P2P é feita em [19]. São abordados itens fundamentais em uma redes P2P, como a proteção de seus recursos e a correta distibuição dos mesmos no ambiente colaborativo. Baseado nas tecnologias JXTA e P2PSockets, o modelo apresentado neste trabalho tem por objetivo garantir a segurança nas redes P2P, assim como estabelecer mecanismos que assegurem o baixo índice de “nós caronas”, que são aqueles que apenas utilizam a rede P2P em benefício próprio, não contribuindo assim para o benefício dos demais *peers*.

Sendo assim, é apresentada a proposta da implantação de mecanismos de controle de acesso, de forma a contribuir para a construção de uma rede P2P segura. Para resolver o problema dos “nós caronas”, são elaboradas técnicas que incentivam a colaboração entre os usuários através de uma fiscalização do comportamento dos peers participantes da rede. A existência de um alto índice deste tipo de nó em uma rede P2P é prejudicial pois aumenta o

congestionamento dos enlaces, concentrando a maior parte dos recursos da rede para os mesmos, em detrimento aos demais.

Desta forma, este trabalho integra os conceitos de computação colaborativa e de controle de acesso, visando a existência de redes P2P mais seguras e justas. Para implementar estes conceitos, o autor apresenta uma aplicação chamada P2P-Control, baseada nos projetos JXTA e P2PSockets.

Uma outra proposta sobre segurança em redes P2P que também concentra suas pesquisas no controle de acesso é encontrada em [20]. Ao contrário de outras trabalhos que se baseiam em entidades centralizadoras para o tratamento das requisições de acesso (o que vai ao encontro do conceito descentralizado das redes P2P), esta proposta apresenta uma arquitetura distribuída para controle de acesso baseado em políticas para grades computacionais (PeGAC). Por ser descentralizada, esta arquitetura possibilita que cada usuário defina a sua política de acesso, independente das escolhidas pelos demais usuários.

Modalidade de processamento distribuído que vem sendo amplamente estudada, a computação em grade é considerada fundamental para a computação sob demanda, pois é base para a virtualização dos recursos [20]. Porém, as soluções baseadas em grades computacionais ainda não são adotadas em grande número nas indústrias e nem mesmo nas universidades, devido a problemas de segurança apresentados. A principal questão de segurança que prejudica a adoção de soluções em grade é o fato de que as várias plataformas de sistemas possuem modelos e mecanismos de segurança pouco eficientes, que não satisfazem aos requisitos principais como autenticidade, confidencialidade, integridade e autorização. E isso tornaria os *peers* participantes deste tipo de grade vulneráveis a ataques como *spoofing*, interceptação e alteração de mensagens e acesso indevido a recursos não autorizados.

Para avaliar esta proposta, o autor incorporou esta arquitetura ao *OurGrid*, *middleware* já existente para a implementação de grades P2P.

5.2 MOBILIDADE

Ao contrário de segurança, mobilidade em redes P2P é um tema bastante novo e, por isso, não existem muitos trabalhos relacionados até o momento. Um importante e recente trabalho sobre o assunto é encontrado em [17], onde a autora apresenta um estudo sobre P2P-Móvel, focando-se principalmente nos desafios existentes para a integração entre as redes P2P e os dispositivos móveis, mas também nas aplicações, protocolos e arquiteturas necessárias para este ambiente.

Em virtude do grande crescimento de dispositivos móveis e da integração dos mesmos com as tecnologias existentes para a comunicação sem fio (Wi-Fi, Bluetooth, etc), há a necessidade do desenvolvimento de aplicações e protocolos que os integre também aos sistemas P2P. Um exemplo é o JXME, uma versão dos protocolos do *framework* JXTA, desenvolvida especialmente para atender aos dispositivos móveis. Quanto às aplicações, podemos citar como exemplos o MobileMule e o PocketSkype, já citados nas seções 4.4.1 e 4.4. 2, respectivamente.

Esta proposta aborda em especial a arquitetura X-Peer, criada recentemente pelo Grupo de Trabalho em Computação Colaborativa (GT-P2P[2]). para atender aos *peers* móveis. Como utilizava basicamente protocolos definidos em XML, apresentava um tempo de processamento muito elevado. Desta forma, o GT-P2P decidiu substituir estes protocolos por

---

[2] GRUPO DE TRABALHO EM COMPUTAÇÃO COLABORATIVA. Disponível em: http://www.gprt.ufpe.br/gtp2p/.

outros no formato binário, reduzindo assim o tempo de processamento, requisito fundamental para dispositivos móveis.

Este trabalho apresenta propostas para a arquitetura X-Peer, de forma a melhor atender aos dispositivos móveis. Para mensurar as melhorias identificadas por esta proposta, a autora desenvolveu uma aplicação que pudesse coletar amostras do tempo de resposta na utilização desta arquitetura.

6 **CONCLUSÃO**

Esta monografia teve por objetivo apresentar as características das redes P2P, assim como suas vantagens, aplicações, restrições e desafios. O seu foco principal, entretanto, os seus principais aspectos de segurança e mobilidade.

O desenvolvimento de novos sistemas P2P é uma tendência de mercado, explicado pelo maior compatilhamento de recursos e informações por parte dos usuários. Isto faz com que os sistemas sejam desenvolvidos para trabalherem de forma distribuída, o que torna essencial a necessidade de segurança das informações.

Um dos principais problemas de segurança enfrentados pelos sistemas P2P é o controle de acesso. Existem propostas para a solução deste problema, mas a grande maioria aborda o controle de acesso centralizado em um único peer da rede, conflitando assim com o principal conceito das redes P2P, que é a descentralização. Por outro lado, novas propostas propondo um controle descentralizado já estão surgindo, utilizando, por exemplo, o conceito de computação em grades. Apesar de também apresentarem alguns problemas que restringem a sua aplicação nas instituições, as grades computacionais estão em constante evolução e, se resolvidos estes principais aspectos de segurança, com certeza serão adotadas como solução para a virtualização e compartilhamento dos recursos computacionais.

Além do controle de acesso, existem algumas questões importantes básicas de segurança que precisam ser solucionadas, como autenticidade, integridade, confidencialidade dos usuários e uma divisão justa dos recursos computacionais entre os mesmos.

Quanto aos aspectos de mobilidade, as redes P2P ainda estão em início de pesquisa. Como os dispositivos móveis e as tecnologias de acesso são relativamente novos no mercado, propostas de protocolos e aplicações que atendam aos mesmos ainda estão em fase de

desenvolvimento e testes. Desta forma, ainda não existe muita bibliografia disponível sobre o assunto.

Acredita-se porém que os sistemas P2P-Móvel são uma forte tendência de mercado, devido ao constante crescimento de dispositivos móveis e aplicativos desenvolvidos para os mesmos. Um fato que comprova esta teoria é o grande e crescente mercado de telefonia celular, apresentando cada vez mais uma grande variedade aparelhos e funcionalidades. O tráfego de dados já é uma realidade entre estes aparelhos, o que nos leva a uma tendência inevitável de compartilhamento de recursos e informações entre os mesmos.

GLOSSÁRIO

Freenet – antigo sistema de troca de arquivos, criado pelo pesquisados Ian Clarke (Universidade de Edimburgo). Neste sistema não há centralização, "clientes e servidor" possuem exatamente a mesma função.

Gnutella – Outro sistema experimental de troca de arquivos que, como a Freenet, realça a descentralização.

Jabber – projeto que combina mensagens instantâneas com o XML.

Napster – famoso e popular sistema de troca de música pela Internet.

Redes Peer-to-Peer (P2P) – redes ponto-a-ponto, caracterizadas pela ausência de em elemento centralizados (como nas redes cliente/servidor). Cada ponto desta rede possui a mesma funcionalidade e poder computacional.

Redes Wireless – rede caracterizada pela ausência de cabos e/ou conectores, onde os dados são trafegados através de radio-transmissão.

SETI@home – projeto anterior ao Napster, que pregava a técnica de distribuição computacional, explorando a enorme quantidade de tempo de inatividade dos computadores pessoais.

Tecnologia da Informação (TI) - conjunto de técnicas, métodos e metodologias que promovem o uso de soluções automatizadas através de um computador.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] O'Reilly and Associates, *O poder transformados das redes ponto a ponto*, editado por Andy Oram, 2001.

[2] ROCHA, João et al, *Peer-to-Peer: Computação Colaborativa na Internet*, Apostila do SBRC, 2004, acessado em www.sbrc2004.ufrgs.br, em 10/05/2005

[3] ROCHA, Rafael R. da, *Redes Peer-to-Peer para compartilhamento de arquivos na Internet*, PEE/COPPE – DEL/POLI – UFRJ, 2003, acessado em www.gta.ufrj.br/~rafael/, em 12/05/2005.

[4] SADOK, Djamel, *GT - Computação Colaborativa (P2P)*, 2003, acessado em www.rnp.br/_arquivo/gt/2003/p2p.pdf, em 12/05/2005

[5] TOWSLEY, Don et al, Modeling Peer-Peer File Sharing Systems, 2003, In: Proceedings of INFOCOMM 2003

[6] SCHOLLMEIER, Rüdiger, "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architetures and Applications", 2002, In: IEEE Internet Computing.

[7] SILVA, M.F.; DIAS, D.S.; *Intenção de Uso de Tecnologia de Informação: um estudo sobre a influência do contexto social em uma empresa do setor acadêmico brasileiro*, Anais do XXXIX CLADEA, 2004.

[8] CLIP2 (2000) "The Gnutella Protocol Specification v0.4", In: http://www.clip2.com/Gnutellaprotocol04.pdf.

[9] MILOJICIC, Dejan S., KALOGERAKI, Vana, LUKOSE, Rajan, NAGARAJA, Kiran, PRUYNE, Jim, RICHARD, Bruno, ROLLINS, Sami, XU, Zhichen, "Peer-to-Peer Computing", technical report, HP Laboratories Palo Alto, Março de 2002.

[10] JXTA Project, http://www.jxta.org, Julho de 2005.

[11] Microsoft, ".NET P2P: Writing Peer-to-Peer Networked Apps with the Microsoft .NET Framework", MSDN Magazine, http://msdn.microsoft.com/msdnmag/issues/01/02/netpeers/, Agosto de 2005.

[12] RIGHI, Rafael et al, *P2P-Role: Uma arquitetura de Controle de Acesso Baseada em Papéis para Sistemas Colaborativos Peer-to-Peer*, LRG/PPGCC – UFSC, 2004/2005

[13] Universidade Federal do Rio de Janeiro, *Redes Peer-to-Peer* - http://www.gta.ufrj.br/grad/04_1/p2p/index.html#Topic21, Agosto de 2005.

[14] McGill Network and Communications Services – *Introduction to P2P Security* - http://www.mcgill.ca/ncs/products/security/p2p/, Agosto de 2005

[15] Grupo de Redes de Computadores – Tutorial do PGP - http://download.unesp.br/documentos/tutoriais/tutorial-pgp.html, Setembro de 2005

[16] Criptografia - http://www.numaboa.com.br/criptologia/lab/quantica.php, Setembro de 2005

[17] OLIVEIRA, Luciana P., *Os dispositivos móveis e as redes peer-to-peer (P2P)*, CIN – UFP, 2005, acessado em www.cin.ufpe.br/~tg/2005-1, em 03/09/2005.

[18] MELLO, Emerson et al, *O uso de SPKI/SDSI em redes P2P*, 2005, In: I Workshop de Redes Peer-to-Peer – WP2P 2005.

[19] RIGHI, Rafael et al, *Controle de Acesso e Combate aos Usuários Caronas em Sistemas Peer-to-Peer*, 2005, In: I Workshop de Redes Peer-to-Peer – WP2P 2005.

[20] SILVA, Juliano F., GASPARY, Luciano P., *PeGAC: Uma Arquitetura de Controle de Acesso baseado em Políticas para Grades Computacionais Peer-to-Peer*, 2005, In: I Workshop de Redes Peer-to-Peer – WP2P 2005.

[21] Napster, http://www.napster.com, Julho de 2005.

[22] SETI Institute, http://www.seti.org, Julho de 2005.

[23] The Free Network Project, http://freenetproject.org, Julho de 2005.

[24] Gnutella Project, http://www.gnutella.com, Julho de 2005.

[25] Jabber Software Foundation, http://www.jabber.org, Julho de 2005.

[26] WIESNER, Stephen*: Conjugate Coding*, 1983, acessado em http://portal.acm.org/citation.cfm?id=1008920 em 24/08/2005.