Controlando Tráfego Peer-to-Peer

Mell Fogliatto, Emerson Virti, Leandro Bertholdo, Liane Tarouco

Ponto de Presença da Rede Nacional de Ensino e Pesquisa do RS – POP-RS
Computer Emergengy Response Team Rio Grande do Sul – CERT-RS
Centro de Processamento de Dados Universidade Federal do RS – UFRGS
Ramiro Barcellos, 2574 – Porto Alegre – RS – Brasil
{mell,emerson,leandro,liane}@penta.ufrgs.br

Abstract: *This article provides an analysis of the main negative aspects of perr-to-peer (P2P) aplications and their efects on the academic network of Rio Grande do Sul (Rede Tchê). We'll present a way to count and classify this kind of traffic by using the software Netflow and the NBAR resource, found in Cisco equipments. This paper also contains a sample of the volume of incidents related to distribution of illegal material registered with the Computer Emergency Response Team Rio Grande do Sul (CERT-RS). The solutions which were adopted by the state academic network and by the Universidade Federal do Rio Grande do Sul (UFRGS) to control traffic P2P will be broached as well. In addiction, two new P2P sistems that facilitate the exchange of information between users will be described.*

Resumo: *Nesse artigo serão analisados os principais aspectos negativos de aplicações peer-to-peer (P2P) e seus efeitos na rede acadêmica do Rio Grande do Sul. Será demonstrada uma forma de classificação e contabilização desse tráfego utilizando o software Netflow e o recurso NBAR existente em equipamentos Cisco. Esse trabalho contém também uma amostra do volume de incidentes relacionados à distribuição de material ilegal registrados junto ao Computer Emergency Response Team Rio Grande do Sul (CERT-RS). Serão também abordadas soluções utilizadas para tratamento do tráfego P2P na rede acadêmica estadual (Rede Tchê) e na Universidade Federal do Rio Grande do Sul (UFRGS). Nesse trabalho também descreveremos dois sistemas P2P que podem beneficiar a troca de informações entre usuários.*

1. Introdução

O uso bastante difundido de aplicações P2P como meio de troca de arquivos MP3 e filmes, por exemplo, causa problemas aos administradores de redes como grande utilização de tráfego e o crescente número de reclamações referentes à violação de Copyright. As inúmeras aplicações e variedades de protocolos utilizados dificulta o controle e/ou bloqueio das mesmas.

Nesse trabalho serão abordados os principais impactos e riscos de tráfego P2P, para a rede e hosts, assim como uma forma de classificação e contabilização desse tráfego. São apresentados dados relacionados à distribuição de material ilegal.

Para mostrar como a arquitetura P2P pode ser utilizada para fins acadêmicos, serão apresentados dois exemplos do bom uso desta, incluindo um sistema de Voz sobre IP

(VoIP) que a utiliza. Finalmente, será explicada a experiência de controle adotada pela UFRGS.

2. Impactos e Riscos

Em 1998, o estudante Shawn Fanning, da Universidade de Massachussets, criou um programa para facilitar a troca de arquivos MP3 com seus colegas – o conhecido Napster. Desde então, esse tipo de programa tem se difundido consideravelmente e inúmeros outros softwares foram criados, dentre eles: Bearshare, BitTorrent, Earthstation, eDonkey, eMule, iMesh, KazaA, MlMac, SoulSeek, WinMX.

Logo quando foi criado o Napster, o bloqueio para as redes P2P era bastante simples. Bastava bloquear o acesso aos servidores que armazenavam os índices de arquivos compartilhados. Após uma melhoria nos protocolos P2P, esses servidores passaram a ser desnecessários e a filtragem do serviço tornou-se bem mais complexa, pois não poderia mais ser feita através do bloqueio dos IPs.

2.1. Vírus, Worms e Spywares

Uma das maiores preocupações atualmente são os vírus e worms que utilizam a rede P2P como meio de propagação.

O primeiro deles foi o Slapper que contaminou mais de 14.000 servidores Linux em 2002 (Symantec). Atualmente existem mais de 300 vírus/worms relacionados às aplicações P2P (Symantec). A maioria deles copia-se automaticamente para os diretórios que contenham a palavra 'SHARE' no nome, normalmente utilizados pelas aplicações em questão. Um exemplo seria o worm W32.HLLW.Sanker que, numa tentativa de aumentar as chances de download/propagação, assume nomes de filmes, programas, cracks, etc. A propagação de vírus via rede P2P é considerada extremamente eficiente e perigosa, já que os arquivos só podem ser verificados após o download completo dos mesmos.

Algumas aplicações, como Kazaa ou iMesh, também oferecem outros tipos de risco para os usuários por, em algumas versões, instalarem spywares acoplados ao programa. Spyware é qualquer programa que monitore ações do usuário na internet e, sem que o usuário tenha conhecimento, transmite-as para um local pré-determinado. São informações normalmente colhidas para fins de propaganda, mas podem ser utilizadas ilicitamente.

2.2. Utilização dos Recursos da Rede

Outro problema é o elevado consumo de banda. Considerando estatísticas pesquisadas, o percentual de banda utilizado por estas aplicações – em redes que não possuem nenhum tipo de controle – pode chegar a 60% de toda a utilização da rede. Um exemplo mais preocupante seria a University of Florida que detectou uma queda de 85% na utilização da rede, após o bloqueio de aplicações P2P.

Como tentativa de contabilizar o consumo de banda, de forma a ter dados mais condizentes com a realidade regional, foram realizados alguns testes.

O primeiro deles consistiu em introduzir na rede uma máquina com uma aplicação P2P disponibilizando alguns filmes e músicas para download. Esse host foi deixado na rede por uma hora e meia e, durante esse tempo, essa máquina conseguiu gerar

aproximadamente 10 Mbps de tráfego, totalizando 16 Mbps. No momento em que o host foi desconectado, o tráfego retorna imediatamente ao normal, ou seja, em torno de 6 Mbps conforme mostra a Figura 1.

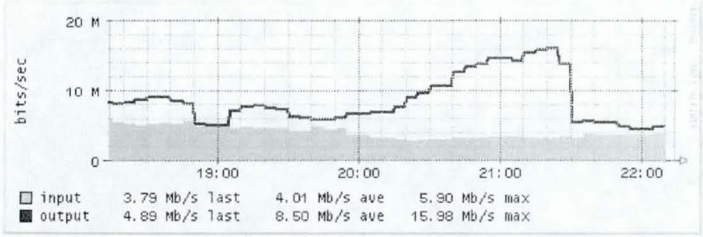

Figura 1. Gráfico demonstrando o tráfego gerado por uma aplicação P2P

A Figura 2 demonstra o impacto das redes P2P no tráfego normal de uma instituição. Às 18:45, é introduzido um filtro na rede e o mesmo é retirado às 19:05. Pode-se constatar uma queda de aproximadamente 3 Mbps.

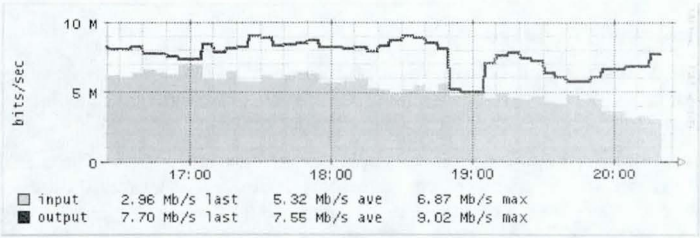

Figura 2. Gráfico demonstrando grande queda de tráfego quando filtradas aplicações P2P

2.3. Incidentes envolvendo distribuição ilegal

Através de um registro das ocorrências relevantes à segurança da rede realizado pelo CERT-RS, a cada trimestre é feita uma análise com base nesses dados e atualmente os incidentes em maior evidência são aqueles relacionados à violação de Copyright, ou seja, distribuição de material ilegal. Notou-se no último ano um aumento considerável nas formalizações de reclamações e denúncias. Isso é demonstrado na figura 3.

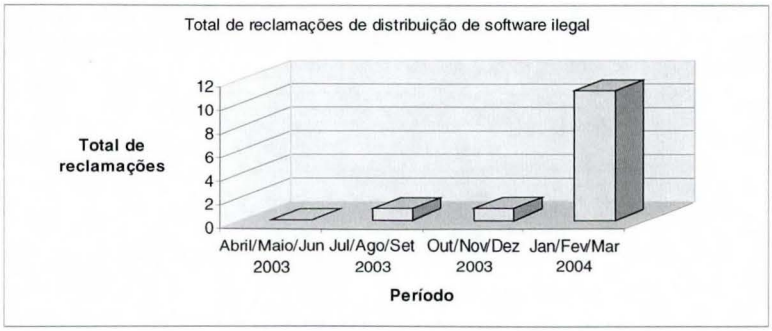

Figura 3. Gráfico demonstrando o aumento de formalizações de denúncias relacionadas à violação de Copyright

Vale ressaltar que algumas instituições americanas chegam a contabilizar cerca de 200 reclamações mensais.

3. Mensurando o Tráfego

Para fins de teste, foi escolhida uma instituição da rede Tchê que não fazia controle sobre aplicações P2P. Um dado significativo é que essa instituição havia dobrado a sua largura de banda – para 8 Mbps – em apenas um ano e meio.

Como a utilização de portas pelas aplicações é dinâmica, foi utilizado para análise o recurso NBAR – disponível em equipamentos Cisco – que, através da análise dos pacotes que trafegam pelo roteador, consegue identificar o tráfego de algumas aplicações P2P, incluindo Blubster, eDonkey, iMesh, Kazza Lite, LimeWire e Morpheus (aplicações testadas pela Cisco Systems). Através desse recurso foi possível implementar uma marcação nos pacotes P2P, utilizando o campo DSCP, para futura análise através do software Netflow. Também foi possível realizar uma filtragem de aplicações P2P no trafego da referida instituição. Os resultados são demonstrados na Figura 4.

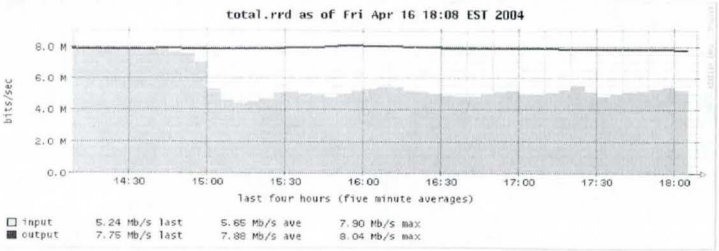

Figura 4. Gráfico demonstrando grande queda no tráfego de entrada quando filtradas aplicações P2P

4. Bom uso de Aplicações P2P

O bom uso da rede P2P permite várias novas aplicações como o XBrain (em desenvolvimento) e o Skype. Ambas serão analisadas a seguir.

4.1. Xbrain

Sistemas como o XBrain, utilizam a estrutura e protocolos P2P para indexar dados dos usuários a partir de servidores localizados na Rede Nacional de Ensino e Pesquisa (RNP). Funciona como um serviço para encontrar pessoas ou grupos que tenham possibilidade de oferecer ajuda em determinadas áreas de conhecimento previamente cadastradas.

As informações são organizadas em meta-dados (apontadores) que indexam dados dos usuários e a localização de recursos. Esses dados são armazenados em dois servidores diferentes, para que não haja possibilidade de perda de informações. Quando os usuários conectam-se em um dos servidores (chamados de XPeer), são mantidos registros de log para que a busca de pessoas seja local e, portanto, mais rápida. Segue ilustração da referida arquitetura.

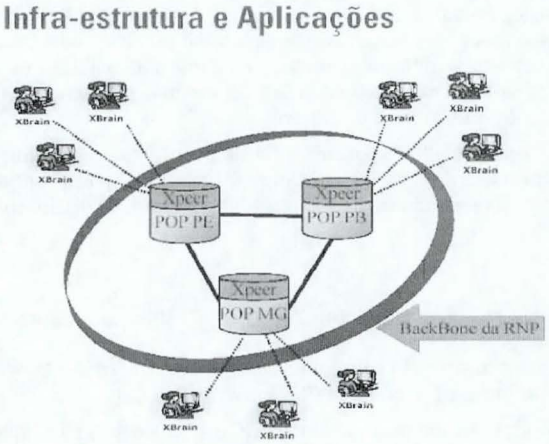

Figura 5. Arquitetura do Sistema XBrain

4.2. Skype

O Skype é um programa de telefonia sobre IP (VoIP) que utiliza a mesma arquitetura P2P do programa KazaA. Os dados dos usuários são armazenados em servidores chamados de supernodes. Quando é feita uma requisição de ligação, o programa busca o nome de usuário requerido na rede e são retornadas as informações necessárias para que se realize a conexão direta entre os usuários. Os dados são cifrados, garantindo privacidade nas conexões.

Possui um protocolo proprietário para transferência de dados onde o uso de portas é randômico, utiliza qualquer porta aberta acima de 1024, caso não encontre nenhuma livre, utiliza a porta 80 (porta normalmente utilizada para tráfego HTTP). O protocolo preferencial é UDP, mas pode utilizar também TCP.

5. A experiência da UFRGS

A solução adotada pela UFRGS baseia-se na conscientização dos usuários da rede acadêmica e no bloqueio dos IPs de máquinas reincidentes. Foi realizada uma reunião com os gerentes das diversas unidades da universidade a fim de divulgar a política de uso aceitável dos recursos computacionais.

O controle é feito através da combinação de scripts que utilizam a ferramenta ngrep para inspeção dos pacotes da rede. Em intervalos de 30 minutos, os scripts são executados e obtém informações das conexões da aplicação KazaA. Apartir dos dados armazenados, são gerados relatórios diários contendo os IPs coletados. Os relatórios são enviados aos gerentes das unidades e esses se encarregam de contactar os usuários a fim de alertá-los e conscientizá-los do impacto causado na rede da universidade. No caso de reincidência, o IP é automaticamente bloqueado. O desbloqueio é realizado através de contato com a Central de Atendimento.

6. Conclusão

Considerando os dados analisados, constatamos que as aplicações P2P são amplamente utilizadas no meio acadêmico e que esse uso (quando direcionado para troca de arquivos áudio-visuais) acarreta significativos problemas, como a diminuição da qualidade da rede, tendo em vista a elevada utilização da mesma, e o crescente número de reclamações de compartilhamento de arquivos ilegais.

Apesar disso, aplicações P2P podem ser benéficas para as instituições da rede acadêmica, se utilizadas com sabedoria. Como foi mostrado, podem ser desenvolvidas aplicações P2P para proporcionar maior interatividade entre os usuários e beneficiar o aprendizado.

Referências:

Extreme Networks, 'Meeting the Peer-to-Peer (P2P) Challenge in Higher Education – An Overview', http://www.extremenetworks.com/common/asp/frameHandler.asp?go=/LIBRARIES/whitepapers/technology/MeetingP2PChallenges_WP.pdf

Extreme Networks, 'Meeting the Peer-to-Peer (P2P) Challenge in Higher Education – A Network Designer's View', http://www.extremenetworks.com/common/asp/frameHandler.asp?go=/LIBRARIES/whitepapers/technology/P2P_NDV_WP.pdf

RNP, Grupo de Trabalho de P2P da RNP, http://www.cin.ufpe.br/~gprt/gtp2p/

Gorgonio Araújo, 'Tecnologias P2P e seu impacto na rede', http://www.rnp.br/_arquivo/sci/2003/p2p.pdf