Swarming: BitTorrent

Redes de Computadores II

Grupo: Ian Freze Cypriano Pires
Matheus Manzoli Ferreira
Paulo Arthur Gonçalves de Lima

Código: TCC00186

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Introdução

- *Peer-to-Peer* (P2P)
  - Conceito
    - final da década 90
  - Pares: Clientes e Servidores
  - Escalabilidade
  - Ausência de Ponto Central de Falhas
  - Pares Transientes
- 43% do tráfego mundial
  - 2008-2009

Introdução

- BitTorrent
  - Bram Cohen
  - 2001
  - Inovações
    - *Swarming* (Enxame)
    - Busca de Conteúdos e Transferência de Dados independentes

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Histórico

- Napster: 1999
  - Shawn Fanning e Sean Parker
  - Primeira rede P2P
  - Híbrido
    - Servidor Central
      - Indexação dos Usuários e seus Conteúdos
- Gnutella
  - Primeira rede descentralizada
  - Busca demorada

Histórico

- Kazaa: 2001
  - “Super Pares”
    - Disponibilidade de Recursos
    - Estabilidade
    - Tempo online
  - Dois níveis hierárquicos
    - Compartilhamento de Conteúdos
    - Indexação de Conteúdos

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

BitTorrent

- Bram Cohen: 2001
- Protocolo para Compartilhamento P2P
- Protocolo da Camada de Aplicação
- Extensões do Protocolo
  - Diminuição de Incompatibilidade
- Código-fonte e Agente de Usuário disponíveis
  - Novas versões de acordo com a necessidade

BitTorrent

- *Swarming*
  - Contribuição do conteúdo antes da conclusão do download
  - Largura de banda de upload e download aproveitadas ao mesmo tempo
- Busca de Conteúdos e Transferência de Dados independentes
  - A busca é na própria internet

BitTorrent

- Comunidades
  - Públicas
    - *Suprnova*
    - *Mininova*
    - *The Pirate Bay*
  - Privadas
    - *BigTorrent*
    - *Bitsoup*

BitTorrent

- Aumento do tráfego
  - Aumento do custo para as ISPs
  - *Traffic Shaping*
    - Desprioriza o protocolo *BitTorrent*

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

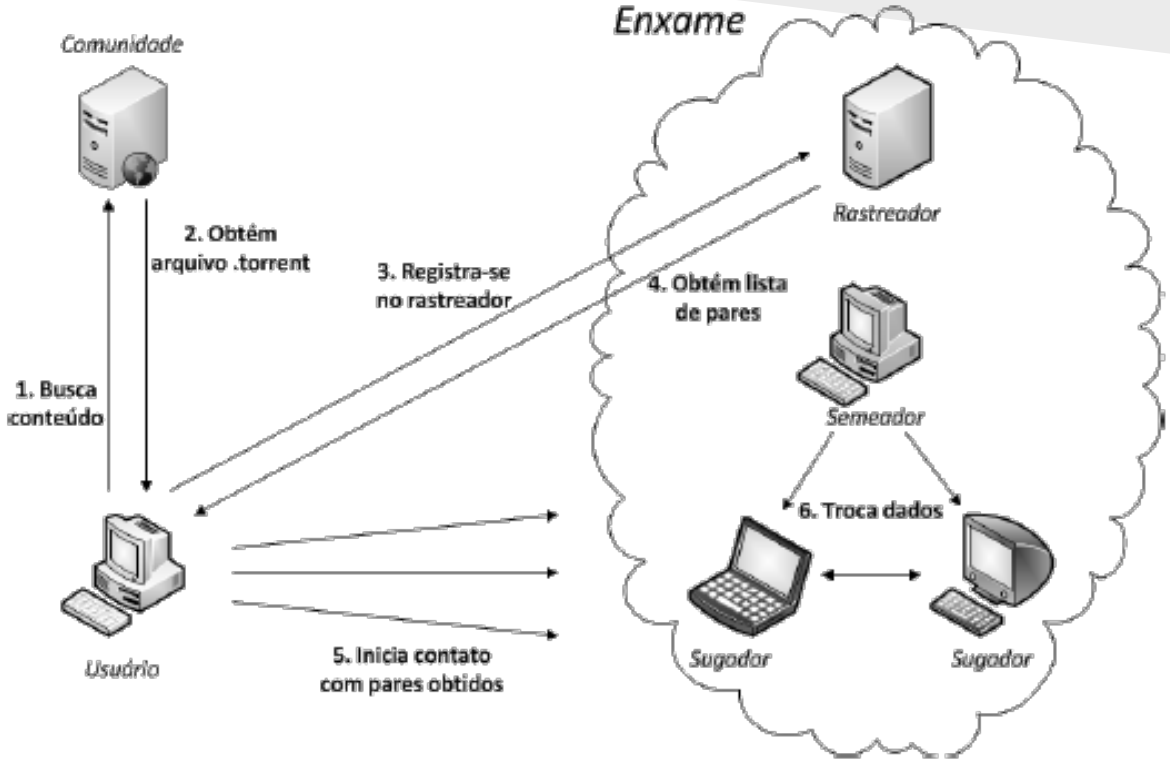
BitTorrent: Funcionamento

- Componentes
  - Enxames
  - Pares
    - Agentes de Usuários
    - 1 ou mais exames
    - Semeador
    - Sugador
  - Rastreadores (*Trackers*)
    - *Peer List* - Lista de IPs de pares
  - Conteúdos

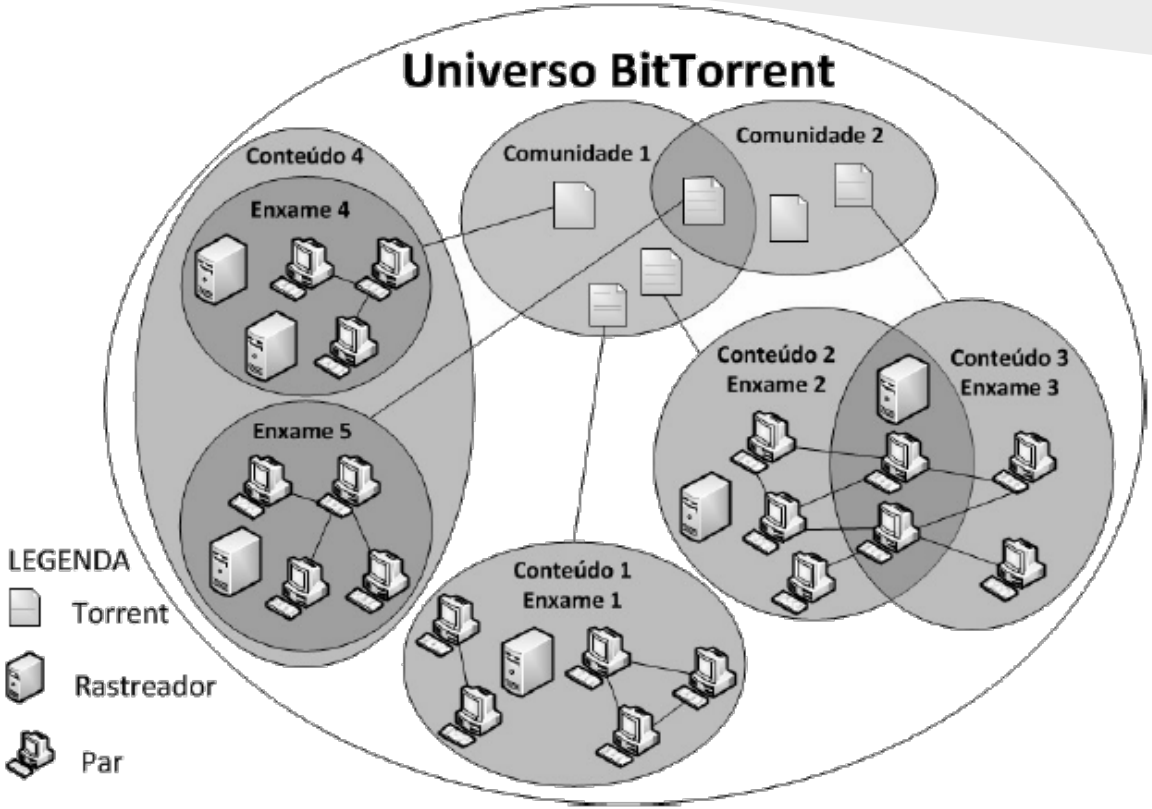
BitTorrent: Funcionamento

- Comunicação com o Rastreador
- Comunicação entre Pares
- Arquivos Metadados (*.torrent)*
  - Peças
  - Blocos

BitTorrent: Funcionamento



BitTorrent: Funcionamento



Comunicação com o Rastreador

- Elemento Centralizado
- Ponto de Encontro entre os Pares
- HTTP/HTTPS
  - HTTP GET
- Lista de Usuários por Enxame
  - Sem obrigatoriedade de comunicação
  - Estimativa

Comunicação com o Rastreador

- Solicitações
  - Atualização do registro do par
  - Resposta contendo n pares do enxame
- *Announce*
- *Scrape*
- 5 casos para solicitações

Comunicação com o Rastreador

- Casos para as solicitações:

1. no início do download, para se registrar na lista do enxame e obter endereços de outros pares;

2. em intervalos regulares, para notificar o rastreador sobre sua presença e obter novos endereços de pares;

3. quando a quantidade de pares ativos cai abaixo de um limite inferior, para obter novos endereços de pares;

4. ao completar o download, para notificar o rastreador que o par se transformou em um semeador;

5. ao deixar o enxame, para notificar sua saída.

Announce

- URL: endereço do rastreador + parâmetros
- Provê estatísticas sobre o enxame
- http://some.tracker.com:999/announce
  ?info_hash=12345678901234567890
  &peer_id=ABCDEFGHIJKLMNOPQRST
  &ip=255.255.255.255
  &port=6881
  &downloaded=1234
  &left=98765
  &event=stopped

Announce

Campo	Descrição
info_hash	identificador único do torrent
peer_id	identificador do par requisitante
port	porta em que o par está escutando por novas conexões
ip	opcional, endereço IP do par
numwant	opcional, número de pares desejados
event	opcional, indica a situação do par no enxame
uploaded	quantidade de upload realizado pelo par
downloaded	quantidade de download realizado pelo par
left	quantidade de dados que faltam para terminar o download
no_peer_id	opcional, permite ao rastreador omitir o id dos pares na resposta
compact	opcional, compreende representação compacta de pares
key	opcional, identificador que só o par e o rastreador conhecem
trackerid	opcional, identifica um par que está retornando ao enxame

Announce: Resposta

Campo	Descrição
peers (dicionário)	lista de pares contendo peer id, endereço IP e porta para cada um
peers (binário)	string da lista de pares usando 6 bytes por par
interval	intervalo em segundos entre requisições regulares feitas pelo par para o rastreador
min_interval	opcional, intervalo mínimo entre requisições
tracker id	string que o par deve enviar de volta nas próximas requisições
failure reason	erro que impossibilitou o atendimento da solicitação
warning message	mensagem de aviso de alguma situação ocorrida
complete	número de semeadores no enxame
incomplete	número de sugadores no enxame

Scrape

- URL: idêntico ao *announce*, porém substituindo por *scrape*
- info_hash: parâmetro único
- Resposta:

Campo	Descrição
files (dicionário)	lista de arquivos requisitados, contendo os campos abaixo para cada um
complete	número de semeadores no enxame
downloaded	número de vezes que o rastreador registrou um término de download
incomplete	número de sugadores no enxame
name	opcional, nome do torrent

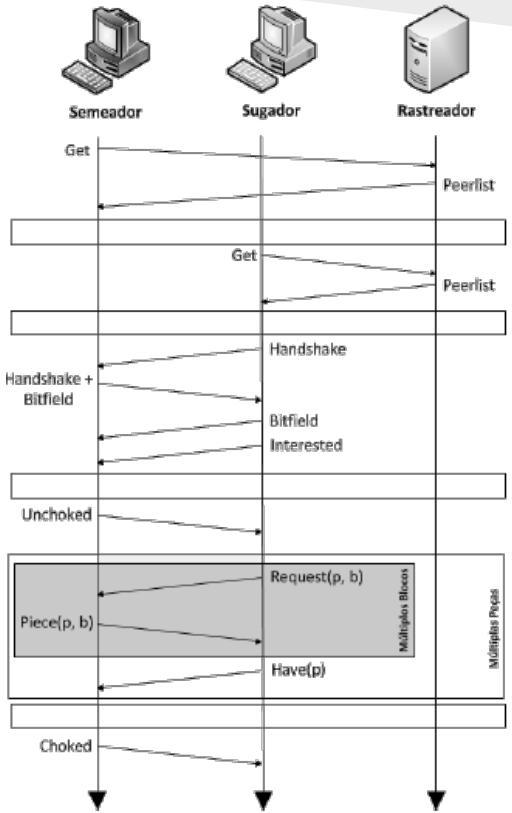
Comunicação entre Pares

- Mensagens entre os pares

Nome	Descrição
keep-alive	notifica que par continua conectado
choke	sinaliza desautorização para requisitar dados (bloqueado)
unchoke	sinaliza autorização para requisitar dados (desbloqueado)
interested	sinaliza interesse (vizinho tem peças que o par local não tem)
not interested	sinaliza desinteresse (vizinho não tem peças que o par local não tem)
have	notifica nova posse de peça
bitfield	mapa de bits que representa as peças possuídas pelo par
request	requisição para um bloco de uma peça
piece	conteúdo em si, correspondente a determinado bloco/peça
cancel	cancela requisição por um bloco de uma peça
port	notifica porta do DHT

Comunicação entre Pares

- Fluxo de Comunicação



Torrent

- Divisão do arquivo em “peças”
  - 256 KB
  - Blocos
    - 16 KB
  - Distribuição Imediata
  - Múltiplos Pares
- Integridade
  - Hash SHA-1
  - Comparação por peças e não por blocos
    - Perda da peça caso um bloco esteja incorreto

Torrent

- Arquivo de Metadados

Campo	Descrição
info	dicionário com a descrição do(s) arquivo(s) do torrent, tais como tamanho de peça, hash das peças, nome e tamanho dos arquivos
announce	URL de announce do rastreador
announce-list	opcional, permite acrescentar mais rastreadores
creation date	opcional, a data de criação do torrent
comment	opcional, comentários do autor
created by	opcional, nome e versão do programa usado para criar o torrent
encoding	opcional, codificação usada para gerar os hashes das peças

Campo	Descrição
piece length	número de bytes em cada peça
pieces	concatenação de todos hashes de cada peça
private	opcional, se ativado, não permite utilizar outras fontes de pares
name	nome do arquivo
files	todos arquivos existentes com os campos a seguir para cada um
length	tamanho de cada arquivo
md5sum	opcional, soma MD5 do arquivo (não é usado)
path	caminho e nome do arquivo

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Políticas e Mecanismos

- Políticas
  - Seleção de Pares
  - Seleção de Peças
- Mecanismos
  - Desbloqueio (Unchoking)
  - Piece Picker

Seleção de Pares

- Seleção de Pares
  - É necessário escolher de quais usuários baixar e para quais enviar.
  - BitTorrent prevê a troca justa - *tit-for-tat*
  - Objetivo: Maximizar taxa de Download e Upload
  - Técnica de Bloqueio ou Engasgamento *(Choking)*
    - Libera Envio (*Unchoke)*
    - Pausa Envio (*Choke*)
    - Cliente escolhe aleatoriamente um para para *Unchoke* - *Optimistic Unchoking*. Descoberta de novos pares eficientes.

Seleção de Peças

- Seleção de Peças
  - Peças podem ser obtidos simultaneamente de vários Pares.
  - Algoritmos utilizados:
    - Prioridade Estrita (*Strict Priority*)
    - *Local Rarest First (LRF)*
    - *Random First Piece*
    - *Endgame*

Políticas e Mecanismos

- Extensões do Protocolo
  - Distributed Hash Table
  - Peer Exchange
  - Local Peer Discovery
  - Fast Extension
  - Superseeding

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Ataques e Contramedidas

- Ataque Sybil - Múltiplas identidades
  - Eclipse
  - Mentira em Massa
  - Corrupção de Peças
- Ataques de Conexão e Largura de banda
- Poluição de Conteúdo
- Contramedidas
  - Nativas do BitTorrent: *Anti-snubbing*, *IP filters*
  - Rotação de Pares, Anti-Corrupção, Reputação, *Funnel*
  - *Closed Swarms*

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Questões Legais e Outros Aspectos

- O Protocolo BitTorrent em si não fere nenhuma lei.
- Arquivos compartilhados freqüentemente são protegidos por direitos autorais e sua troca é, portanto, ilegal.
- Os Servidores de Rastreamento é um ponto de conflito, já que seus responsáveis argumentam que não estão armazenando nenhum conteúdo ilegal.
- As corporações antipirataria os acusam de facilitadores.

Questões Legais e Outros Aspectos

- Problemas:
  - Poucos Seeds no Swarm -> Redução da velocidade de download.
  - Sumiço de conteúdo através do tempo. Torrentes sem seeds.
  - Consumo de quase toda largura de banda.

Questões Legais e Outros Aspectos

- Apesar do compartilhamento ilegal de músicas, vídeos e etc. existem ainda diversas aplicações legais para redes BitTorrent.
- Muitos programas de código aberto optaram por distribuir suas versões novas através do BitTorrent.
- Companhias desenvolvedoras de Jogos adotaram a plataforma BitTorrent DNA para distribuir as atualizações e correções de forma rápida e barata.

Sumário

- Introdução
- Histórico
- BitTorrent
- Funcionamento
- Políticas e Mecanismo
- Ataques e Contramedidas
- Questões Legais e Outros Aspectos
- Conclusão

Conclusão

O BitTorrent é um protocolo extremamente útil para troca de arquivos, graças a introdução do conceito de Enxame e a desassociação dos mecanismos de busca com os de transferências. Não é exagero considerar o BitTorrent uma grande invenção. Uma tecnologia bastante funcional, criativa e que evolui com o passar do tempo.

Swarming: BitTorrent

Redes de Computadores II

Grupo: Ian Freze Cypriano Pires
Matheus Manzoli Ferreira
Paulo Arthur Gonçalves de Lima

Código: TCC00186

Perguntas

1) Por que o Napster não conseguiu sobreviver, assim como o BitTorrent?

2) 1 vantagem e 1 desvantagem de se ter muitos blocos por peças.

Respostas

1) Porque era o próprio Napster que indexava os conteúdos, o mesmo sabia qual conteúdo o usuário possuía, assim foi alvo de muitas ações judiciais. Com o BitTorrent, a responsabilidade fica com as comunidades.

2) Vantagem: cada bloco pode ser solicitado por um par distinto.

   Desvantagem: Diminuiria o enxame, pois para compartilhar a peça é necessário ter todos os blocos da peça.