Peer to Peer and Overlay Networks
The impact of P2P file sharing traffic on the Internet

Ricardo Lopes Pereira
ricardo.pereira@inesc-id.pt

IST

28-11-2011
1 Motivation

2 The ISP’s perspective

3 Drafting behind Akamai
   - Overview
   - Algorithm
   - Evaluation

4 Biased Neighbor Selection
   - Overview
   - Implementation
   - Evaluation

5 ALTO
   - Overview
   - Details
   - Current proposals
Motivation

The ISP’s perspective
Drafting behind Akamai
Biased Neighbor Selection
ALTO

Dominating types of traffic on the Internet

1 CacheLogic Research: Peer to Peer in 2005
Weight of P2P

Ipoque: Internet Study 2007

2
Motivation
The ISP’s perspective
Drafting behind Akamai
Biased Neighbor Selection
ALTO

Daily usage pattern

³Ipoque: Internet Study 2007
Motivation
The ISP’s perspective
Drafting behind Akamai
Biased Neighbor Selection
ALTO

P2P adoption

Relative User Numbers per Protocol Type

<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Germany (University)</th>
<th>Middle East</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P</td>
<td>18%</td>
<td>20%</td>
</tr>
<tr>
<td>VoIP</td>
<td>30%</td>
<td>7%</td>
</tr>
<tr>
<td>IM</td>
<td>17%</td>
<td>17%</td>
</tr>
<tr>
<td>http</td>
<td>99%</td>
<td>94%</td>
</tr>
<tr>
<td>DDL</td>
<td>9%</td>
<td>17%</td>
</tr>
<tr>
<td>Streaming</td>
<td>23%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Ipoque: Internet Study 2007
Dominant applications

P2P Protocol Distribution by Volume

<table>
<thead>
<tr>
<th>Region</th>
<th>BitTorrent</th>
<th>DirectConnect</th>
<th>Gnutella</th>
<th>eDonkey</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>29%</td>
<td>79%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>29%</td>
<td>79%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Southern Europe</td>
<td>57%</td>
<td>29%</td>
<td>2%</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>Middle East</td>
<td>39%</td>
<td>39%</td>
<td>9%</td>
<td>3%</td>
<td>0%</td>
</tr>
<tr>
<td>Australia</td>
<td>14%</td>
<td>14%</td>
<td>9%</td>
<td>3%</td>
<td>0%</td>
</tr>
</tbody>
</table>

5Ipoque: Internet Study 2007
Types of transferred files

Traffic Volume per Content Type
Germany, BitTorrent

- Video 79.17%
- Movie 37.24%
- TV 21.15%
- Porn 13.05%
- Anime 7.09%
- Music 7.78%
- Application 4.97%
- Game 5.77%
- Software 10.74%
- eBook 0.81%
- Audio 9.19%
- Picture 0.09%
- eBook 1.41%

6

Ipoque: Internet Study 2007
Cost/benefit analysis

Cost:
- The capacity exhaustion may force the ISP to upgrade its network, increasing its costs
- When links are charged using 95th percentil, it may increase costs significantly
- The congestion caused by P2P impacts other application, causing customers to complaint

Benefits:
- Motivates users to subscribe to wideband services
- Compels users to upgrade to faster access speed whenever these become available
A different problem

- P2P traffic does not have a well define source, unlike HTTP traffic where a set of large sites is known. Caches are difficult to install and link dimensioning is complicated.
- P2P traffic is continuous on the short term. Users stop to read a webpage before downloading the next.
- P2P traffic is continuous on the long run as no user presence is required. It prevents ISPs from taking advantage of daily usage patterns to optimize their networks, particularly global networks that cover several time zones.
P2P traffic is symmetric. In the client-server model (HTTP, NNTP) the client is a consumer of information, not a producer.

P2P may result in the exchange of copyrighted material, which may represent unlawful competition to other services from the ISP (triple play).
Question

How do ISPs deal with the previous issues?
ISPs’ response

- Low upload rate. Will globally reduce the download rates. Due to reciprocity, will lower the download rate into the ISP’s network
- Place traffic limits (total or distinguishing among national and international traffic). The potential costs of P2P will discourage users
- Use specialized P2P caches and redirect P2P traffic to these caches
- Bandwidth throttling to limit the weight of P2P traffic: at all times or only during congestion
- Bandwidth throttling to limit heavy hitters’ traffic: lower a user’s bandwidth after he exceeds a certain traffic amount or period of time
- Upgrade link capacity
Limitations of these responses

- Low upload rates: it will also impact other applications, hindering the use of video-conferencing, slow sending emails with large attachments, uploading photos or videos, ...
- Traffic limits: will impact other applications as well. Limits the attractiveness of the higher bandwidth commercial offers
- Use of caches: potential legal liability, ISPs will perform the download, storage, sharing and transmission of copyrighted material. Could be construed as assisting/promoting copyright violations
Limitations of these responses

- Caches and bandwidth throttling: require deep packet inspection. Impossible with encrypted traffic.
- Caches and bandwidth throttling: violate network neutrality principals by treating different traffic types differently.
- Caches and bandwidth throttling: violate the user privacy by reading application data.
- Capacity upgrades: P2P file sharing applications are designed to use as much bandwidth as possible.
In order to operate correctly, each user must obtain one full copy of the shared file. There is no way to reduce this minimum (other than compressing data).

However, the closer it comes from, the fewer links are crossed.

If each packet crosses fewer links, on average, there will be fewer packets going through each link.

The research on minimising the negative impact of P2P file sharing traffic on the Internet has focused on the locality of the sources:

- by fetching data locally, either from the same ISP or from a peering ISP, the costs for the ISP are significantly reduced.
- the reduction of the number of hops crossed by each data packet will reduce congestion.
<table>
<thead>
<tr>
<th>Motivation</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ISP’s perspective</td>
<td>Algorithm</td>
</tr>
<tr>
<td>Drafting behind Akamai</td>
<td>Evaluation</td>
</tr>
<tr>
<td>Biased Neighbor Selection</td>
<td></td>
</tr>
</tbody>
</table>

ALTO

Ono

Ricardo Lopes Pereira

Peer to Peer and Overlay Networks
Overview

- System for choosing close-by peers to exchange data with
- Works with BitTorrent
- Uses Akamai to determine which of the available peers are close
- Implemented as an Azureus plugin, was downloaded by hundreds of thousands of users
Akamai - Overview

- Akamai is a content distribution network (CDN)
- Uses over 25,000 servers placed at the edge of the Internet, typically in local ISP’s datacenters
- Forwards data using an overlay network in order to avoid congestion and increase availability and throughput (like RON)
- Servers use hard disk drives to deploy local caches
- ISP’s customers are served locally or from the closest servers which already own the required content
- Uses DNS to guide client to the most suitable server
- Akamai network continuously performs measurements which allow it to have a precise view of the conditions of the Internet
Motivation
The ISP’s perspective
Drafting behind Akamai
Biased Neighbor Selection
ALTO

Overview
Algorithm
Evaluation

Akamai - DNS

Website name is CNAME to Akamai name
Server chosen using: website name (content) and client’s IP (or of its DNS server)
The closest server, with the required content and light load, is returned

---

*“Drafting Behind Akamai”, AoJan Su, David R. Choffnes, Aleksandar Kuzmanovic and Fabián E. Bustamante*
Algorithm

- Consider two clients to which the same Akamai server is assigned to be close to each other.
- Periodically, peers perform DNS resolutions to Akamai sites.
- Each peer calculates a “ratio map” with the frequency it is assigned to each server: \( \mu_a = \langle (r_k, f_k), (r_l, f_l), ..., (r_m, f_m) \rangle \).
- Cosine similarity is used to define the proximity among two peers:
  \[
  cos\_sim(a, b) = \frac{\sum_{i \in I_a} (\mu_{a,i} \cdot \mu_{b,i})}{\sqrt{\sum_{i \in I_a} \mu_{a,i}^2 \cdot \sum_{i \in I_b} \mu_{b,i}^2}}
  \]
  - 0 if there are no common servers and 1 if the servers and frequencies are the same. Peer are considered to be close if \( \geq 0.15 \).
- Ratio maps exchanged by the Ono plugin or stored in a DHT.
- Tries to determine values for peers which do not use Ono by performing DNS queries on their behalf.
Disadvantages

- Selected peer may not be in the same ISP
- Depends on the Akamai network, without paying for that service
Scenario

- Azureus plugin gathers statistical data:
  - Rate (upload and download), every 5s
  - RTT to other peers (ping)
  - Paths to other peers using traceroute

- Compare values for the peers selected by the plugin against the average case (does not take into account the effect of the reciprocity algorithm)
Path length

![Graphs showing CDF of path length](image)

7“Taming the Torrent”, David R. Choffnes and Fabián E. Bustamante
Delay and loss

8“Taming the Torrent”, David R. Choffnes and Fabián E. Bustamante
Average download rate improves by 31% and upload by 42%.

"Taming the Torrent", David R. Choffnes and Fabián E. Bustamante
The ISP on the left favours local traffic. The one on the right treats traffic uniformly, hurting the performance of Ono as it limits the number of peers available for the reciprocity system to use.

10 “Taming the Torrent”, David R. Choffnes and Fabián E. Bustamante
Biased Neighbor Selection

11 The images presented in this section are from “Improving Traffic Locality in BitTorrent via Biased Neighbor Selection”, Ruchir Bindal, Pei Cao, William Chan
Main goal: to limit the traffic among ISPs by favouring the exchange of file content between peer within the same ISP.

Works by forcing BitTorrent client to communicate mainly with peers within the same ISP.

When it communicates with the tracker, peer will mainly learn of other peers within the same ISP.

May be implemented at the tracker or using a firewall/traffic shapper.

There is still a set of peers external to the ISP, in order to ensure that the download terminates.
Implementation - Tracker

- Tracker responds so that of the 35 peers return, $35 - K$ belong to the same ISP.
- When tracker does not know enough peers within the same ISP, it will request the peers to reask for more peers soon.
- Three methods are suggested to identify peers within the same ISP:
  - The use of topology maps or IP to AS mappings
  - Cooperation by ISPs which would supply their IP ranges
  - Indication, by the peer, in the HTTP request header, of the ISP’s identifiers. This would likely be user configurable
- Disadvantages: requires trackers and clients to be modified
Implementation - Traffic shaper

- Implemented at traffic shapers (TS) by the ISP’s edge routers
  - TS observes communication with the trackers, getting to know peers inside the ISP belonging to each file swarm
  - TS manipulates HTTP replies from trackers, replacing outside peer by internal peers

- Whenever new local peers appear, the TS may reset ongoing outside connections, forcing the peers to perform a new tracker query

- Advantages:
  - Does not require changes to either the tracker or the clients
  - May be put into operation by a single ISP without requiring user cooperation
Disadvantages

- It only works when there is a sufficient number of peers inside the ISP exchanging the same file:
  - Offers little results for small ISPs
  - Will only work for the most popular files
  - When traffic shapers are used by large ISPs (which will require a large number of TSes) the communication among these may be significant
  - Will have difficulties if encrypted traffic is used, as well as with peer exchange and DHTs
Scenario

- Evaluation using a specifically developed simulator which provides a very high level abstraction of the network
- 14 ISPs, each with 50 clients
- Clients have 100Kb/s upload and 1Mb/s download
- ISPs are all connect among each other
- ISPs have no capacity limit among themselves
- Each ISP present a global data rate limit to/from all the others. This is intended to simulate the use of a traffic shaper
- High bandwidth (symmetrical) nodes where introduced, directly connected to all the ISPs. These were intended to represent peers at universities and companies
- Study focused on flash crowd
- Evaluated criteria: download time, redundancy - number of copies entering each ISP (from 1 to 50)
BNS vs traffic shaping

- In the first table 1.0 represents 5312s
- Seed had 400Kb/s upload
- Expected redundancy
  \[ N \times (1 - N/G) = 50 \times (1 - 50/700) = 46.4 \] with
  \( N \) - peers within the ISP, \( G \) - total number of peers
- Bottleneck forces tit-for-tat into preferring internal peers

<table>
<thead>
<tr>
<th>ISP bottleneck</th>
<th>50th percentile</th>
<th>95th percentile</th>
<th>traffic redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>no bottleneck</td>
<td>1.0</td>
<td>1.35</td>
<td>46.9</td>
</tr>
<tr>
<td>2.5Mbps</td>
<td>1.43</td>
<td>1.59</td>
<td>31.76</td>
</tr>
<tr>
<td>1.5Mbps</td>
<td>2.01</td>
<td>2.05</td>
<td>24.88</td>
</tr>
<tr>
<td>500kbps</td>
<td>3.33</td>
<td>3.53</td>
<td>21.65</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Neighbor Selection</th>
<th>50th percentile</th>
<th>95th percentile</th>
<th>traffic redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular BT</td>
<td>5,312</td>
<td>7,152</td>
<td>46.72</td>
</tr>
<tr>
<td>Biased ( k = 1 )</td>
<td>5,168</td>
<td>6,206</td>
<td>3.44</td>
</tr>
<tr>
<td>Biased ( k = 5 )</td>
<td>5,172</td>
<td>6,281</td>
<td>9.74</td>
</tr>
<tr>
<td>Biased ( k = 17 )</td>
<td>5,220</td>
<td>5,872</td>
<td>21.38</td>
</tr>
</tbody>
</table>
Download time CDF for traffic shaping

CDF curves for Download Times

- no bottleneck
- 2.5 Mbps
- 1.5 Mbps
- 500 Kbps

% of peers finished vs. Time (ms)
Download time CDF for BNS

CDF curves for Download Times

- Regular BT
- Biased, k = 1
- Biased, k = 5
- Biased, k = 17

% of peers finished vs. Time (ms)
Conclusions

- BNS provides better results for ISPs with small costs for users
- BNS may be combined with traffic shaping. In this case the advantages are even more significant as BNS provides local peers to be used, avoiding the bottleneck
Application Layer Traffic Optimization$^{12}$

$^{12}$Images from “Traffic Localization for P2P-Applications: The ALTO Approach” by Jan Seedorf, Sebastian Kiesel and Martin Stiemerling
History

- The several works published on P2P traffic locality lead IETF to recognize the importance of cross-layer cooperation in the context of P2P communications.
- On May 2008 a workshop on P2P infrastructures was held, where 3 complementary work areas were identified:
  - QoS provisioning - not pursued
  - New approaches to congestion - a new workgroup was created: Low Extra Delay Background Transport
  - Traffic locality - a new workgroup was created: Application Layer Traffic Optimization (ALTO)
Goals

- Main goal: design a query-response protocol for the ALTO service, which P2P applications may use to obtain information to guide them in performing better than random peer selection.

- Win-win scenario for both customers and ISPs: customers should benefit from higher performance, ISPs should lower their costs (e.g. lower inter-ISP traffic).
Current state

- Workgroup has just defined the problem statement
- A few individual proposals already exist
Usage scenario

Application overlay topology

Physical topology

Peer 1

Peer 2

Peer 3

Client Application Protocol

ALTO service

Query

ALTO Guidance

From ISP:
- Static topology information
- Operational costs
- Policies

Routing state information

Resource

Resource
Scope

- Does not define how the ALTO server receives the information
- Does not define the protocols of the applications using it
- Only defines the communication protocol between the ALTO server and the ALTO client
- Covers security, privacy and service discovery issues
Direct usage by the client

- Client contacts the ALTO service of its ISP
- The network view is shared by both
- Server may be announced using DHCP or PPP options
Usage by intermediate

- Example: BitTorrent tracker
- ALTO server and ALTO client may have different views of the network
- ALTO client may communicate with several ALTO servers
- Servers could be discovered using DNS
Motivation

For ISPs:
- Greater control over the traffic going through their networks
- Cost reduction
- Congestion reduction

For users:
- Faster downloads
- Lower costs due to the selection of peers reachable through cheaper paths (e.g. when the ISP charges differently for national and international traffic)
- It’s essential to ensure that users adopt ALTO, otherwise it will not succeed
Obstacles

- **Privacy:**
  - ISP might be reluctant to divulge information which allows the structure of its network and peering agreements to be inferred.
  - User might not want to reveal who its “partners in crime” are. It may simply consider that information to be private.

- **Trust:**
  - ISP’s ability to manipulate the client, forcing it to perform the download from saboteur peers.
  - Even though ISPs may have to gain or be pressured to manipulate clients, users will abandon the service should they believe this practice to affect them.

- The effort involved in processing each request may turn ALTO servers into easy denial-of-service targets.
Steps common to all the proposals

- The application, using its protocol, finds a set of peers which are capable of providing a service.
- The application contacts the ALTO client (may be itself), supplying the list of possible peers. The ALTO client and server, together determine the best candidates.
- The ALTO client returns the list of suitable peers to the application, together with advise. Advise may be expressed by ordering or scoring peers.
- The application combines the advices received from ALTO with its local preferences and contacts peers. It may contact ALTO again at any time, should it not be pleased with the choices.
Motivation
The ISP’s perspective
Drafting behind Akamai
Biased Neighbor Selection
ALTO

Proposals

**Proxidor**
Uses the oracle model. Application supplies list of IPs. ALTO server returns it sorted according to preference

**P4P**
ALTO client downloads network maps (sets of network regions and respective parameters). It's up to the client to perform its decision using this data
Proposals

H12

Tries to balance the two previous models in regard to privacy and amount of data that has to be transferred. Client may supply set of regions (instead of IP addresses). The server may reply with courser or finer detail according to its information security policy.
The end

Questions?