Peer-to-Peer Traffic

Masood Khosroshahy

August 2009

Tech. Report

Contents

1 Peer-to-Peer Protocols Classification

Peer-to-Peer (P2P) systems/protocols have gained enormous popularity since 2001, due to technological as well as social/cultural reasons. The technological driving force behind P2P systems is related to lack of scalability and reliability of centralized architectures in simultaneously serving a huge number of clients due to a near-insatiable global demand for digital content. Although there are many legitimate uses of P2P technology, free sharing of copyrighted content has been arguably the deciding social/cultural factor behind the huge success and popularity of P2P systems. In what follows, we briefly classify the important P2P protocols that have emerged, some of which have already vanished, in this relatively short period of time.

While there are few number of classification methods available for P2P systems, we focus on the most cited classification method which is based on the degree of centralization and reflects the chronological order of appearance of P2P systems. P2P protocols can be roughly divided into three generations with "streaming media over third generation systems" potentially forming the forth generation.

Napster and DirectConnect are notable examples of the first generation of P2P systems which adopted the centralized architecture. According to this architecture, there were few servers in the overlay network which took control of the tasks of indexing contents in connected peers (end-hosts or end-users) and informing each peer regarding how to reach other peers to get the interested piece of content. As the peers joined and left the network, servers kept track of online connected peers (and their contents) and provided this up-to-date information to connected peers upon request. The servers provided the functionalities of searching for any specific content upon request by a peer and returning a list of peers who own the content. The peer then connected directly to those peers who host the content to receive it. First-generation P2P systems provided too much functionality to be scalable as well as to escape the legal ramifications of illegal sharing of copyrighted material.

The demise of first generation centralized P2P systems was quickly followed by second generation decentralized P2P systems. Gnutella is the prominent example of second generation P2P systems which was architected based on a complete decentralized approach with all the functionalities such as content insertion and distribution and exchanges of control messages handled by peers,

i.e. no single point of authority and coordination. Peers which initially joined the overlay network acquired the addresses of other peers using specific techniques including from a peers list shipped by the software itself. Peers then used query flooding to find out about other peers and searched for contents by sending queries to their neighbors which in turn contacted their own neighbors, with a certain threshold in the level depth. As soon as a match was found, the reverse path was traversed and the original querying peers contacted directly the peers which possessed the respective contents. While second generation decentralized systems clearly bypassed the legal hurdles, they nevertheless failed due to scalability issues as the share of passed control messages in the network grew exponentially as the overlay network grew in size.

The third generation of P2P systems, known as hybrid P2P systems, combines the strength of centralized and decentralized systems, examples of which include FastTrack, BitTorrent, eDonkey and latest versions of Gnutella. In the hybrid architecture, there are designated "super nodes" which form an upper layer in the overlay network serving the lower layer which is comprised of ordinary peers. Super nodes are responsible for routing search queries, keeping peers and contents lists, providing these lists upon request of ordinary peers, providing statistics, etc. and have varied functionalities depending on the type of P2P system. The functionalities of these super nodes are also carefully tailored and scaled down to narrowly avoid the legal problems which brought down the first generation systems. In these hybrid systems, an ordinary peer finds and contacts a super node and asks for the content. The super node then returns the list of peers which possess the respective content and the querying peer in turn contacts the peers from that list directly to obtain the content, whether as a whole or in pieces/chunks and whether from a single peer or in parallel from a number of peers. Third generation hybrid P2P systems therefore exhibit improved robustness and have low overhead in terms of passed controlled messages. Furthermore, ordinary web techniques are often utilized to aid peers to find contents and super nodes which translates into further reduction of signaling messages.

2 Traffic Characteristics: An Overview

In this section, we report on the analysis that we have done of the published studies [1–11] about (or including) peer-to-peer traffic characterization. The goal of the analysis that has been carried out was to find a common ground between the reported P2P traffic characteristics.

As mentioned in many of the aforementioned studies [1–11], the share of P2P traffic in general, and BitTorrent in particular, is enormous in the overall traffic flowing in the Internet. This has strongly motivated a research into characteristics of this traffic so that the network operators could plan their architectural evolution in the long-term and their network management policies in the short-term with more insight.

In a recent comprehensive study of P2P traffic characteristics [10][1], authors have measured and identified the P2P traffic (based on transport level information) on a trans-pacific link between Japan and the US. They have then analyzed and modeled the marginal distributions of the traffic volume, connection duration and connection inter-arrival times for several P2P applications (Napster, BitTorrent, eDonkey, Gnutella and Fasttrack). The most significant finding of the study has been the fact that the traffic of each P2P application exhibits different characteristics which has been attributed to the different strategies employed and the different parameters chosen in each P2P application. Therefore, the traffic metric (per-connection traffic volume, connection duration and connections inter-arrival times) cannot be characterized uniformly with a single probability distribution model across various types of P2P applications.

An interesting citation from [10] could be the fitted model for the traffic volume of BitTorrent. According to the measurement results, a typical Complementary Cumulative Distribution Function (CCDF) of the traffic volume contributed by a single BitTorrent connection follows extremely well the Weibull distribution. As the Probability Density Function (PDF) of a Weibull-distributed random variable is $f(x) = abx^{b-1}e^{-ax^b}, x \geq 0$ (with two parameters $a > 0, b > 0$), the parameters chosen to fit the measured CCDF into the Weibull distribution are $a = 0.0097$ and $b = 0.3843$.

Among the three metrics, i.e. per-connection traffic volume, connection duration and connections inter-arrival times, the first two show huge differences across the five P2P applications. For example, most Napster connection are less than 1Kbytes and last less than 10 seconds, on the other hand, more than 30% of BitTorrent connections are more than 100 Kbytes and last hundreds of seconds; authors attribute these differences to the chosen file block size in each P2P application. The last metric, connections inter-arrival times, however, is reported to be about the same for all P2P applications. Connection inter-arrival times of less than 1 second are attributed to the P2P client initiating different connections to transfer the content, while the tail of the distribution is attributed to the user thinking time. This behavoir implies that P2P clients act more or less the same with re-

[1] Note that other cited studies on P2P traffic characteristics also report more or less the same results, however, the studies have not been done as comprehensive as in [10].

gard to the frequency of connection initiation and that the users' behavior, in terms of thinking/idle time, is also largely the same across the P2P applications.

As mentioned in [10], understanding of stochastic properties of the Peer-to-Peer traffic could benefit traffic control algorithms. However, as the measurements have been done in some core link in the network in all the carried out studies, this understanding might only help P2P traffic shaping equipments deployed in the same core link. In the P2P traffic analyses, we would be interested to know the geographical distribution of hosts participating in a P2P overlay network. Such a study could reveal valuable information regarding how origin/destination traffic matrix in the design of networks should evolve to take into account the nature of the P2P traffic. Similarly, such a study could benefit the design of Application Layer Traffic Optimization (ALTO) (see Section 4) mechanisms. Unfortunately, such studies are extremely rare. A notable example would be [12], in which it is shown that the traffic of a P2P application, "eDonkey 2000", has interest-based and geographical clustering. We expect the same behavior with regard to the BitTorrent traffic: some files, like linux distributions are distributed globally (interest-based), while a video clip about some celebrity in a town might attract a flash crowd from that geographical area only.

3 Traffic Identification

Classification of applications in the Internet remains a challenging task. Use of transport-layer port numbers and packet payload inspection are increasingly unreliable approaches to classify applications [13]. Applications often use randomly-selected port numbers and increasingly implement some sort of payload encryption to remain in the shadows and undetected by network profilers and traffic shapers. Furthermore, the sheer number of new applications (including P2P applications) and the fact that most of them are poorly-documented present an insurmountable challenge to reverse engineering efforts in designing traffic classifiers based on payload inspection approaches. Novel approaches have been proposed to effectively classify traffic based on flow connection patterns and without inspection of the payload [14–17].

In [14–16], the authors describe certain P2P flow patterns which can be detected using simple state machines and have shown a high degree of accuracy in the identification of the P2P traffic. For example, a simple pattern of flows that has a high probability of belonging to P2P traffic is that when a source/destination IP pair is detected to have concurrent UDP and TCP connections (with

UDP connection commonly used for control messages and the TCP one for content transfer).

In the case of BitTorrent, clients can operate on any port number including port numbers of traditional Internet applications like HTTP's 80. This behavior renders port-based traffic identification methods useless and has given rise to payload-based identification methods [18]. However, BitTorrent applications are now employing payload encryption methods to avoid detection. The encryption is effective due to the fact that payload string matching misses all encrypted P2P packets. BitTorrent clients can use "Message Stream Encryption" [19] which is an encapsulation protocol, designed to provide a random-looking header and payload[2].

The primary reason for current interest in identification of Peer-to-Peer traffic is improving the performance of P2P traffic shapers deployed in the core network. While their performance has improved significantly in recent years [20], the P2P traffic filters have had to play catch-up with the latest trends in the P2P development, remaining one step behind most of the time.

4 Application Layer Traffic Optimization: The Current Proposals

There have been a number of initiatives to address the congestion problems caused by P2P traffic for network operators. These proposals mostly revolve around the idea of routing P2P packets differently, compared to other packet types, as a result of cooperation between ISPs and P2P software developers, while preserving each party's interest to some extent in the process (lower congestion/cost for ISPs and acceptable speed/performance for P2P developers and users). Furthermore, there have been few caching solutions for P2P traffic which will be introduced as well. In what follows, we present the state-of-the-art in this area.

4.1 P4P: Proactive network Provider Participation for P2P

P4P [21–23], which stands for Proactive network Provider Participation for P2P, is a framework based on which end-host applications and network providers have an explicit communication. As a result, knowing the end-users status (location in the network topology, etc.), network operators'

[2]Payload encryption is optional; payload may be in plaintext format or it may use a strong encryption mode which is RC4. RC4 is the most widely-used software stream cipher, use of which can be found in a de facto security protocol like SSL

policies and various link-specific costs, applications can participate in the resource optimization of the operator's network.

The P4P framework is made possible using a central entity, called "iTracker", deployed and configured by the network operator. "iTracker" provides information about the network topology and operator policies to querying entities such as end-host P2P applications (i.e. the BitTorrent client) and P2P network's centralized elements[3](i.e. BitTorrent's Torrent Tracker). P2P peers query the iTracker to obtain information regarding preferred routes and the costly routes to avoid. They then use that information in their peer selection algorithms to lower the costs incurred by the network operator[4]. A P2P-based content distributer, who wishes to distribute its content to the subscribers of an ISP, will receive two pieces of information from the iTracker: 1) "Points of Presence (PoPs)" of subscribers 2) The cost of using the link between each pair of PoPs (peering cost). Using this information, the P2P network elements (peers and trackers) try to minimize the overall cost of distribution of the content among the peers.

4.2 Ono

Ono [25] is a software service that allows peers to identify other nearby peers rather efficiently, without any need for an ISP to get involved (by installing an iTracker for example, as in the P4P case). The approach is simple and works as follows. Ono queries existing Content Distribution Networks (CDNs) and based on the returned information decides whether or not two peers are nearby. If two peers are assigned to the same CDN server, it is likely that the two peers are geographically close, hence better fits to trade content pieces with each other. Specifically, the Ono plugin enables the peer selection algorithm in a BitTorrent client to find peers which are closest in terms of number of traversed hops to reach each other. Note that while Ono is suggested to be an effective service, its operation is entirely dependent on the queried commercial CDN servers. Ono plugin is just a simple way to relay the information from CDN servers to the BitTorrent clients; it does not independently try to evaluate the closeness of the peers.

[3]Called appTrackers in P4P terminology.

[4]P4P Working Group [24] has been conducting field tests with the participation of Yale University, Pando Networks (configuring/operating the P4P's P2P network entities), Verizon and Telefonica (both network operators, configuring/operating the P4P's iTracker entity). The reported field test results show improved performance on both sides: lower congestion/cost for the network operator and higher speed for the P2P application.

4.3 Caching Mechanisms

CacheLogic's Cachepliance series [26] and Joltid's PeerCache product [27] came to market few years ago, but failed to attract attention. In what follows, we briefly explain the logic behind their operation[5]. Cachepliance incorporated large amounts of storage along with caching and software which prevented unnecessary flow of traffic out of the network. The content was locally cached and served on demand from a local entity. Cachepliance intercepted download requests from inside the network, thereby reducing network operator's transit bandwidth requirements. Likewise, Cachepliance intercepted download requests from outside the network, thereby reducing bandwidth use and congestion on the local access network. They have also conducted field tests with NTL (a network operator) and BitTorrent and showed its effectiveness to meet the stated objectives. Joltid's PeerCache worked similar to Cachepliance, however, it was designed, tested and optimized for FastTrack P2P protocol (responsible for the bulk of the P2P traffic at the time - 2003).

4.4 ISP Oracles

Caching solutions are legal landmines considering that the cache provider (i.e. the network operator) may seem to be "facilitating" illegal exchange of copyrighted content. To address this issue, an oracle-based solution provided by ISPs has been proposed in [28, 29], which is conceptually similar to the P4P initiative discussed before. The idea is helping the P2P client make better decisions when choosing which peers to trade content pieces with. For that, the P2P client contacts an ISP-operated server, an "oracle", and sends a list of potential peers that it wants to connect with. The oracle then processes the list and returns an ordered list back to the P2P client. In ordering the peers list, the oracle takes into account all the parameters that are of importance to the ISP to reduce its costs as well as the congestion caused by the P2P traffic[6]. The P2P client then uses the received ordered list in its peer selection algorithm, which leads to a near-optimal solution mitigating the problems due to the P2P traffic. Both simulation and measurement results show improvements in

[5] Strictly speaking, caching mechanisms should not be categorized under ALTO mechanisms, as caching is usually provided by the network operator without permission/cooperation/awareness of end-hosts (the current choice is made to avoid overly-complicated categorization.). The term "ALTO mechanism" generally refers to a kind of mechanism in which end-hosts (i.e. P2P client applications) actively get involved in the optimization of the use of network resources.

[6] Considered parameters include (but not limited to): 1) geographical location of the peer, if the ISP prefers to keep its traffic local 2) bandwidth links of the peers (and preferring the clients with higher bandwidth links), since that information about its clients is readily available to the ISP, but harder to derive by distant client-based measurements.

P2P clients' download time and reduction in the overall P2P traffic. Note that while this solution is effective, some modifications should be done to the P2P clients which needs the cooperation of the P2P developers in its implementation.

Similar to the above method, another oracle-like service has been proposed recently: "ISP-Driven Informed Path Selection (IDIPS)" [30, 31]. IDIPS has been developed, as a service provided by the network operator, to respond to client queries requiring performance and path information. Clients send to the IDIPS their source and potential destination addresses along with a Differentiated Services CodePoint (DSCP), meaning that the client expresses the Quality of Service that it expects to receive. Like the oracle solution discussed before, ISP orders the "paths" according to some parameters (lowering costs, avoiding congestion, providing the requested QoS, etc.) and returns the ordered list back to the querying client. The client then processes the list and proceeds to choose some peers to interact with. Authors have also provided some measurement results, proving the effectiveness of their proposed mechanism.

4.5 BitTorrent DNA

Like the introduced "Caching Mechanisms", "BitTorrent DNA" [32], the latest development concerning BitTorrent, cannot be seamlessly categorized under the ALTO mechanisms. However, its design goals partially overlap with the goals of ALTO mechanisms; hence its introduction here as we conclude this report.

"BitTorrent Delivery Network Accelerator (DNA)" technology has been introduced as the BitTorrent Inc. company[7] adopted a "legitimate" business model by catering for the content distribution needs of the big businesses[8]. Being a proprietary technology, there is no publication regarding the details of the technology. In what follows, we briefly summarize what is known about BitTorrent DNA.

DNA leverages existing servers (CDNs) to seed a privately-managed peer network coordinated by a specialized tracker. A client who wishes to download a content, which is distributed using

[7] The company founded by the original inventor of the protocol, Bram Cohen. Note that the BitTorrent client distributed by BitTorrent Inc. is not necessarily the most popular client, as the protocol has been implemented in numerous other open-source and commercial applications.

[8] A Content Distribution Network (CDN) company called Brightcove was the first client of BitTorrent DNA; a company that powers the content delivery needs (mostly video streaming) of companies such as CBS, Discovery Channel, Disney, Reuters, Warner Music Group, Sony and Fox.

DNA, is served in parallel from both the server resources of the CDN and the managed peer network to meet the QoS level of the specific content. When a user installs a BitTorrent client, a DNA client is also installed automatically. Afterwards, as soon as the user clicks and requests to download a DNA-enabled content, the URL to that content is passed to a proxy at BitTorrent Inc. The user's DNA client is subsequently introduced to the DNA peers, who are currently downloading that same content, by a tracker operated by the company.

Addressing the negative impact of the BitTorrent traffic both on the users' own applications and on the network, the company has incorporated some mechanisms, details of which have remained largely unpublished; here is what we know about these mechanisms: The DNA client, installed in the user's computer, monitors the usage of the Internet connection by other applications as well (VoIP, Web Browsers, etc.) and limits the bandwidth consumed by the BitTorrent client in order to preserve the performance of other applications. On the network side, DNA tries to minimize the negative impact of the BitTorrent traffic by using a peer selection algorithm that takes locality of the remote peers into account and prefers peers that are away as few hops as possible. Furthermore, it tries to discover and utilize the local BitTorrent cache, if deployed in the network. Finally, BitTorrent DNA has replaced TCP with a proprietary UDP-based bandwidth management protocol for content transfer between peers.

5 UARA

[This section is added to this Tech Report in 2011 to mention a paper due to its relevancy]

Masood Khosroshahy (2011), *"UARA in edge routers: An effective approach to user fairness and traffic shaping"*, International Journal of Communication Systems (Wiley), doi: 10.1002/dac.1262

Abstract:

The ever-increasing share of the peer-to-peer (P2P) traffic flowing in the Internet has unleashed new challenges to the quality of service provisioning. Striving to accommodate the rise of P2P traffic or to curb its growth has led to many schemes being proposed: P2P caches, P2P filters, ALTO mechanisms and re-ECN. In this paper, we propose a scheme named "UARA:User/Application-aware RED-based AQM" which has a better perspective on the problem: UARA is proposed to be implemented at the edge routers providing real-time near-end-user traffic shaping and congestion avoidance. UARA closes the loopholes exploited by the P2P traffic by bringing under control the P2P users who open and use numerous simultaneous connections. In congestion times, UARA monitors the flows of each user and caps the bandwidth used by "power users" which leads to the fair usage of network resources. While doing so, UARA also prioritizes the real-time traffic of each user, further enhancing the average user quality of experience (QoE). UARA hence centralizes three important functionalities at the edge routers: (1) congestion avoidance; (2) providing user fairness; (3) prioritizing real-time traffic. The simulation results indicate that average user QoE is significantly improved in congestion times with UARA at the edge routers.

Uara resources available from: http://www.masoodkh.com/uara/

References

[1] Stefan Saroiu, P. Krishna Gummadi, and Steven D. Gribble. A measurement study of peer-to-peer file sharing systems. In *Proceedings of Multimedia Computing and Networking 2002 (MMCN'02)*, San Jose, CA, January 2002.

[2] S. Ohzahata and K. Kawashima. A study on traffic characteristics evaluation for a pure p2p application. In *Proc. 16th Euromicro Conference on Parallel, Distributed and Network-Based Processing PDP 2008*, pages 483–490, 2008.

[3] Sung-Don Joo, Chae-Woo Lee, and Yeon Hwa Chung. Analysis and modeling of traffic from residential high speed internet subscribers. pages 410 – 19, Busan, South Korea, 2004.

[4] S. Sen and Jia Wang. Analyzing peer-to-peer traffic across large networks. *IEEE/ACM Transactions on Networking*, 12(2):219–232, 2004.

[5] David Erman, Dragos Ilie, and Adrian Popescu. Bittorrent traffic characteristics. In *Proc. International Multi-Conference on Computing in the Global Information Technology ICCGI '06*, pages 42–42, Aug. 2006.

[6] Chun-Ying Huang and Chin-Laung Lei. Bounding peer-to-peer upload traffic in client networks. In *Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks DSN '07*, pages 759–769, 2007.

[7] N.B. Azzouna and F. Guillemin. Experimental analysis of the impact of peer-to-peer applications on traffic in commercial ip networks. *European Transactions on Telecommunications*, 15(6):511 – 22, 2004.

[8] T. Mori, M. Uchida, and S. Goto. Flow analysis of internet traffic: World wide web versus peer-to-peer. *Systems and Computers in Japan*, 36(11):70 – 81, 2005.

[9] P. Olivier. Internet data flow characterization and bandwidth sharing modelling. In *Managing Traffic Performance in Converged Networks. Proceedings 20th International Teletraffic Congress, ITC20 2007*, pages 986 – 97, France Telecom, 2007.

[10] Guanghui He, Jennifer Hou, Wei-Peng Chen, and Takeo Hamada. One size does not fit all: A detailed analysis and modeling of p2p traffic. In *Proc. IEEE Global Telecommunications Conference GLOBECOM '07*, pages 393–398, 26–30 Nov. 2007.

[11] Md. Naimul Basher. Characterization of peer-to-peer and web traffic at a network edge. Master's thesis, The University of Calgary, June 2007.

[12] F. Le Fessant, S. Handurukande, A.M. Kermarrec, and L. Massoulié. Clustering in peer-to-peer filesharing workloads. In *Proc. IPTPS'04*, pages 217–226, San Diego, CA, Feb. 2004.

[13] A. Madhukar and C. Williamson. A longitudinal study of p2p traffic classification. In *Proc. 14th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems MASCOTS 2006*, pages 179–188, 2006.

[14] Thomas Karagiannis, Andre Broido, Michalis Faloutsos, and Kc claffy. Transport layer identification of p2p traffic. In *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, pages 121–134. ACM, 2004.

[15] Thomas Karagiannis, Konstantina Papagiannaki, and Michalis Faloutsos. Blinc: multilevel traffic classification in the dark. In *SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 229–240. ACM, 2005.

[16] Thomas Karagiannis. *Novel Techniques and Models for Network Traffic Profiling: Characterizing the Unknown*. PhD thesis, University of California Riverside, June 2006.

[17] Jeffrey Erman, Anirban Mahanti, Martin Arlitt, Ira Cohen, and Carey Williamson. Offline/realtime traffic classification using semi-supervised learning. *Performance Evaluation*, 64(9-12):1194 – 1213, 2007. Performance 2007, 26th International Symposium on Computer Performance, Modeling, Measurements, and Evaluation.

[18] Subhabrata Sen, Oliver Spatscheck, and Dongmei Wang. Accurate, scalable in-network identification of p2p traffic using application signatures. In *WWW '04: Proceedings of the 13th international conference on World Wide Web*, pages 512–521. ACM, 2004.

[19] Message stream encryption specification.
`http://www.azureuswiki.com/index.php/Message_Stream_Encryption`.
Consulted on June 15, 2008.

[20] Carsten Rossenhövel. Peer-to-peer filters: Ready for internet prime time?
Internet Evolution Technical Report, March 2008.
`http://www.internetevolution.com/document.asp?doc_id=148803`.

[21] Pando networks (p4p working group co-founder and co-chair).
`http://www.pandonetworks.com/p4p`. Consulted on February 05, 2009.

[22] Haiyong Xie; Ph.D. Candidate; Yale University. P4p publications.
`http://cs-www.cs.yale.edu/homes/yong/p4p.html`. Consulted on February 05, 2009.

[23] P4p informational (inc. field test results) website.
`http://www.openp4p.net/`. Consulted on February 05, 2009.

[24] Dcia p4p working group. http://www.dcia.info/activities/#P4P. Consulted on February 05, 2009.

[25] Ono plugin for the vuze (azureus) bittorrent client.
`http://www.aqualab.cs.northwestern.edu/projects/Ono.html`.
Consulted on February 04, 2009.

[26] Cachelogic's cachepliance 1000 & 4000 series product specification documents (2004).
`http://www.cachelogic.com`. Consulted on January 20, 2009.

[27] Joltid peercache product specification document (2003).
`http://www.joltid.com/documents/PeerCache_Information.pdf`.
Consulted on January 20, 2009.

[28] Vinay Aggarwal, Anja Feldmann, and Christian Scheideler. Can isps and p2p users cooperate for improved performance? *SIGCOMM Comput. Commun. Rev.*, 37(3):29–40, 2007.

[29] V. Aggarwal, O. Akonjang, and A. Feldmann. Improving user and isp experience through isp-aided p2p locality. In *Proc. INFOCOM Computer Communications Workshops IEEE Conference on*, pages 1–6, 2008.

[30] D. Saucez, B. Donnet, and O. Bonaventure. Idips : Isp-driven informed path selection. IETF Internet-Draft [draft-saucez-idips-01.txt], November 2008. (Work in Progress).

[31] Damien Saucez, Benoit Donnet, and Olivier Bonaventure. Implementation and preliminary evaluation of an isp-driven informed path selection. In *CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference*, pages 1–2. ACM, 2007.

[32] Bittorrent dna technology. `http://www.bittorrent.com/dna/technology/`. Consulted on February 09, 2009.