

A Router-aided P2P Traffic Localization Method with Bandwidth Limitation

Hiep Hoang-Van, Takumi Miyoshi, *Member, IEEE*, and Olivier Fourmaux, *Member, IEEE*

Abstract—Recently, peer-to-peer (P2P) systems generate a large amount of unwanted cross-domain traffic on the Internet due to a lack of knowledge about physical network topology. The unwanted cross-domain traffic is especially costly for the internet service providers (ISPs). To reduce the cross-ISP/AS (autonomous system) traffic, the existing approaches introduce network-aware strategies in which a lot of modifications of P2P systems are required. In particular, each P2P application must be modified to integrate with a locality-aware procedure and/or a communication protocol to obtain the topological information from an “oracle” server. In this paper, we propose two schemes for localizing P2P traffic without any peer reaction: (1) fixed-length bandwidth limitation scheme, (2) hierarchical bandwidth limitation scheme. By intentionally limiting the bandwidth of each connection path between peers based on geographical location of the peers destinations, the traffic can be localized with single level for the first scheme and with multiple levels for the second scheme. Compared to the existing locality-enhancing approaches, our two schemes require neither dedicated servers, nor cooperation between ISPs and users, nor any modification of existing P2P application software. Therefore, we believe that all types of P2P applications can easily utilize our proposals. Experiments on P2P streaming applications indicate that the fixed-length bandwidth limitation scheme successfully realizes P2P traffic localization. Moreover, the hierarchical bandwidth limitation scheme not only significantly reduces the cross AS/ISP traffic but also maintains a good performance of P2P applications.

Index Terms—P2P, router-aided approach, hierarchical traffic localization, bandwidth limitation.

I. INTRODUCTION

MOST P2P applications form overlay networks for communicating among peers on top of the physical network topology. However, the overlay is often established based on the resource availability and thus largely independent from the underlay network topology. As a result, P2P systems generate a large quantity of unwanted traffic on the Internet. In particular, the unwanted cross-domain traffic proves to be costly for the ISPs. Therefore, the ISPs or network operators often manage P2P traffic by bandwidth throttling or limiting and/or even blocking P2P systems in their network. On the contrary, the P2P systems try to hide them from the network by changing their design, e.g., applying dynamic port strategies. It is more challenging to recognize the P2P traffic. In addition, blocking P2P systems would reduce sharply the demand of

end users, who have family with using some P2P applications. Therefore, the fundamental concern of the ISPs is essentially not to block, but to turn the inter-ISP/AS traffic into the intra-domain traffic.

To address the problem, a variety of methods have been proposed, and many works confirmed that the consideration of peer location would reduce the cross-domain traffic as well as conserve the bandwidth. However, almost all of existing approaches solve the problem on the application layer. Therefore, P2P systems must be essentially equipped with a locality-aware neighbor peer-selection mechanism to realize traffic localization. This can be achieved by one of the following ways:

- The enhancement of trackers to efficiently gather information of the underlay network. On the P2P applications side, they need to implement an appropriate protocol to communicate with the enhanced trackers.
- The modification of the P2P application software to upgrade from the current neighbor peer-selection mechanisms to locality-aware ones. Because P2P applications currently only employ random and/or round-trip time (RTT)-based strategies.
- Or both of the above.

Several modifications of P2P systems are inevitable as described above.

In this paper, we introduce a novel approach to localize P2P traffic without any modification of existing application software. We exploit an important feature of P2P applications that a querying peer will select a candidate peer as its neighbor if the candidate peer is likely to provide better performance. For instance, the querying peer tends to select a candidate peer who has shorter RTT than others. Since the network performance is affected by various factors, communication with peers across network domains is sometimes better than the local communication. This leads to the increasing of cross-domain traffic. Based on this observation, if we intentionally degrade the quality of connection paths of inter-domain traffic, the querying peer will tend to remove the inter-domain connections and select the local connections instead. In other words, we can turn the inter-domain traffic into the intra-domain traffic. To achieve this, we propose to limit the bandwidth of the inter-domain traffic at network routers.

We propose two different schemes: (1) fixed-length bandwidth limitation scheme; (2) hierarchical bandwidth limitation scheme. In the first scheme, the bandwidth of all the connections to foreign peers will be limited with a constant value. This scheme is to demonstrate the effectiveness of the bandwidth limitation in traffic localization problem. In the

H. Hoang-Van and T. Miyoshi are with the Graduate School of Engineering and Science, Shibaura Institute of Technology, Saitama-shi, Saitama, 337-8570 Japan.

O. Fourmaux is with the Laboratoire d'Informatique de Paris 6, UPMC Sorbonne Universités, Paris, 75005 France.

Manuscript received ???; revised ???.

second scheme, the traffic can be hierarchically localized with multiple levels of localization such as inside an AS, inside an ISP, or inside a country. The value of limited bandwidth should depend on both the physical distance between peers and the number of peers exists in the same area as the querying peer. The first factor ensures that lower bandwidth will be allocated for farther peers than closer ones, whereas the second factor realizes our hierarchical feature of localization. In particular, we first try to localize the traffic at AS level if some candidate peers exist inside the same AS. We will change from AS level to ISP and country level if no candidate peer exists in the same AS and ISP, respectively. Since our proposal is deployed on network routers outside of the peers, it is completely independent of P2P applications, and thus requires neither dedicated servers, nor collaboration between ISPs and P2P users, nor modification of application software. Therefore, the proposal can be easily applied to all P2P applications.

The remainder of this paper is organized as follows. In Section II, we discuss about the related work. Section III describes two proposed schemes for hierarchical traffic localization, and Section IV then shows the implementation two schemes. The experimental results are presented in Section V. Finally, Section VI provides conclusions and our future work.

II. RELATE WORK

Overprovisioning and deep packet inspection (DPI)-based bandwidth management are considered the best conventional strategies to deal with P2P traffic [1]. However, they do not solve the fundamental concern of the ISPs, which is to reduce the cross-domain traffic, i.e., to localize the traffic. The idea of P2P traffic localization was first introduced by Karagiannis et al., who studied BitTorrent trace logs and found that about 50 percent of the files could be downloaded from peers at the same ISP if a locality-aware peer-selection mechanism is used [2]. Plissonneau et al. analyzed eDonkey file sharing system, and reported that most of traffic traversed nationwide or international networks, in which 40 percent of the traffic could be localized [3].

Aggarwal et al. proposed a solution to build up a relationship between ISPs and P2P users [4]. ISPs maintain an “oracle service to help P2P users in selecting their neighboring peers. When a P2P user sends a list of possible neighbors to the oracle, the oracle ranks them according to certain criteria such as high bandwidth links, low latency, or closer peers, etc. Although the oracle can be introduced into the network independently of the P2P applications, this scheme requires a dedicated server as well as a good cooperation between ISPs and P2P users. In addition, each P2P application must be modified to add an additional protocol to communicate with the oracle.

P4P is a famous framework that follows the oracle idea [5]. In P4P, ISPs maintain iTrackers in their own networks. The iTrackers provide the p-distance interface, representing the logical distance between each pair of PIDs (aggregation nodes). There are several dimensions for the ISPs to control the p-distance information. From the P2P applications side, they can obtain the necessary information for neighbor peer

selection directly from the iTrackers or indirectly via app-Trackers. Recently, the Internet Engineering Task Force (IETF) has standardized a query/respond protocol for the oracle-based system in rfc5693 and rfc6708, known as Application Layer Traffic Optimization (ALTO) [6], [7]. Although the ALTO approaches improve not only the network efficiency but also the P2P application performance, they require dedicated servers and several modifications of existing P2P application software.

Choffnes and Bustamante proved that the presence of the oracle service provided by ISPs is redundant because the content distributed networks (CDNs) have already gathered all necessary information [8]. By using CDNs DNS redirection, they hypothesized that two peers are recognized as close to each other if they are sent to a similar set of replica servers. This idea is implemented as a java plugin to Azureus BitTorrent client, named “Ono. This method requires support from many subscribing peers installing Ono plugin distributed worldwide. Furthermore, to apply this method for other types of P2P applications such as P2P streaming applications (P2PTV), we believe that some modifications must be required.

Bindal et al. proposed biased neighbor-selection scheme applying for BitTorrent in which a peer selects only k peers from outside of the ISP, and the majority peers within the same ISP as itself, where k is a parameter [9]. This biased neighbor-selection scheme successfully reduces inter-domain traffic while maintain the near-optimal performance of the BitTorrent, i.e., it realizes a win-no lose situation. The authors also introduced two ideas for implementing the biased neighbor selection: (1) the enhancement of trackers and clients and (2) the use of P2P traffic shaping devices. The former certainly requires a lot of software modification, whereas the latter requires no modification of trackers or clients but does require knowing the peer list format sent from the trackers. In other words, the method depends on the P2P applications.

Lee and Nakao introduced another approach for traffic localization applying to BitTorrent, called Netpherd, which is independent of the application [10], [11]. Netpherd tries to enable local peers to communicate with each other by adding artificial delay into the inter-domain traffic. The idea of degrading network performance of inter-domain connections is similar to our work. However, they focused on BitTorrent, a file sharing system. Moreover, Netpherd only localizes the traffic at AS level because the delay length is constant for all inter-AS traffic, e.g., 100 ms.

We previously proposed P2P-DISTO for P2P traffic localization without any peer reaction, which focused on P2PTV services [12]. P2P-DISTO inserts an additional delay into each P2P packet according to geographical locations of peers. The delay length is constant for all foreign traffic, e.g., 500 ms or 1000 ms, P2P-DISTO thus only realizes traffic localization at country level. In this study, we proceed to follow P2P-DISTO but use a different mechanism. We limit the bandwidth of the inter-domain traffic instead of inserting delay. In addition, we extend the scope of localization from single level to multiple levels.

III. PROPOSED SCHEMES

According to the report of Cisco System Inc. [13], the P2P traffic is on the declining in percentage of overall Internet traffic due to the degradation of P2P file sharing systems. However, it is still increasing rapidly in volume with tremendous growing of video streaming services. Therefore, our goal is to realize traffic localization focusing on P2PTV services, which are predicted to be much more popular in the very near future. Thus, currently, P2PTV applications such as PPTV (update version of PPLive) [14], PPStream [15], SopCast [16], Zattoo [17] have become increasingly popular.

The majority of existing P2PTV applications implements RTT-based peer-selection mechanism. In particular, P2PTV tends to eliminate worse connections based on the RTT measured before starting downloads the data pieces. From this observation, we proposed two different schemes based on bandwidth limitation. Since the RTT information can be changed by limiting the bandwidth, we influence the neighbor peer selection of P2PTV indirectly.

Given a querying peer, $peer_0$, and a list of N candidate peers, $\{peer_1, peer_2, \dots, peer_N\}$, let (as_0, isp_0, cc_0) be denoted AS number, ISP name, and country code of the querying peer, respectively, and (as_i, isp_i, cc_i) be denoted AS number, ISP name, and country code of $peer_i$, respectively. Our goal is to compute the limited bandwidth assigned to a candidate $peer_i$.

A. Fixed-length bandwidth limitation scheme

To prove the effectiveness of bandwidth limitation method in P2P traffic localization problem. We first introduce fixed-length bandwidth limitation scheme. Figure 1 presents the concept of the scheme. The scheme does nothing with local traffic inside the same country as the querying peer, but limits the bandwidth of traffic that goes out to or comes in from different countries. In other words, the bandwidth of connections with foreign peers is forced to be much lower than that of local ones. The RTTs of the foreign peers is thus increased. The querying peer will then prefer to connect with local neighboring peers that have shorter RTTs.

The limited bandwidth assigned to a candidate $peer_i$ is computed by [kbps], as follows:

$$bw_i = f(cc_i, cc_0) = \begin{cases} +\infty, & \text{if } cc_i = cc_0 \\ C, & \text{if } cc_i \neq cc_0 \end{cases} \quad (1)$$

where C is a constant number.

B. Hierarchical bandwidth limitation scheme

Localizing the traffic at country level only is surely not enough in real situation. We therefore introduce a hierarchical bandwidth limitation scheme for localizing traffic hierarchically with multiple levels. Figure 2 illustrates the concept of the scheme at AS level. We do nothing with local traffic within the same AS, but limit the bandwidth of the traffic that goes out to or comes in from different ASes, ISPs, or countries. For farther peers, a lower bandwidth is allocated than closer ones. We will change from AS level to ISP and country level if no candidate peer exists in the same AS and ISP, respectively. The behavior of the ISP level is as follows: do nothing with

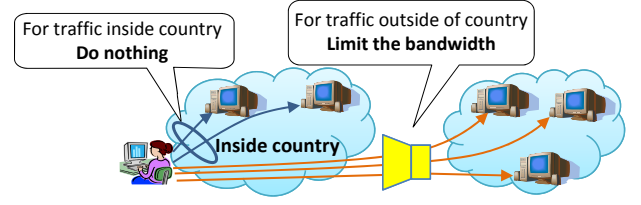


Fig. 1: The concept of fixed-length bandwidth limitation scheme.

the traffic within the same ISP, but limit the bandwidth of the traffic that goes out to or comes in from different ISPs, or countries. Similarly, for the country level, we do nothing with the traffic inside the country but limit the bandwidth of overseas traffic.

To realize the concept of hierarchical traffic localization mentioned above, we propose a logical distance representing a distance adjustment factor between a candidate peer and the querying peer. The logical distance between $peer_i$ and $peer_0$ is defined as follows:

$$D_i = f_1(as_i, as_0)e^{-\frac{1}{n_1+\varepsilon}} + f_2(isp_i, isp_0)e^{-\frac{1}{n_2+\varepsilon}} + f_3(isp_i, cc_i, isp_0, cc_0)e^{-\frac{1}{n_3+\varepsilon}}, \quad (2)$$

where n_1 , n_2 , and n_3 are the total numbers of peers in the same AS, ISP, and country as $peer_0$, respectively, ε is a very tiny constant to ensure the denominators of all fractions never come to zero, and

$$f_1(as_i, as_0) = \begin{cases} 0, & \text{if } as_i = as_0 \\ \theta_1, & \text{if } as_i \neq as_0 \end{cases} \quad (3)$$

$$f_2(isp_i, isp_0) = \begin{cases} 0, & \text{if } isp_i = isp_0 \\ \theta_2, & \text{if } isp_i \neq isp_0 \end{cases} \quad (4)$$

$$f_3(isp_i, cc_i, isp_0, cc_0) = \begin{cases} 0, & \text{if } isp_i = isp_0 \\ d(peer_i, peer_0), & \text{if } isp_i \neq isp_0, \\ & \text{and } cc_i = cc_0 \\ \theta_3 + d(peer_i, peer_0), & \text{if } cc_i \neq cc_0 \end{cases} \quad (5)$$

Since ISPs, including ASes, have to manage their own networks, the information that the querying peer connects to a peer exists inside or outside the AS/ISP is the most important. Hence, θ_1 and θ_2 are coefficients to differentiate the inter-AS/ISP traffic from the intra-AS/ISP traffic, respectively. To ensure that the logical distances of farther peers will be higher than those of closer ones, we define $d(peer_i, peer_0)$ as the physical distance between $peer_i$ and $peer_0$. Even though some nearby physical locations might be far apart from each other in terms of network connectivity in some specific cases, the physical distance is still a reasonable estimation in most cases. The coefficient, θ_3 , is to make the distances of foreign peers sufficient higher than those of local ones.

Since lower bandwidth should be allocated for farther peers, we compute the limited bandwidth for a candidate $peer_i$ as follows:

$$bw_i = \frac{1}{D_i + \varepsilon_1} \times B[\text{kbps}], \quad (6)$$

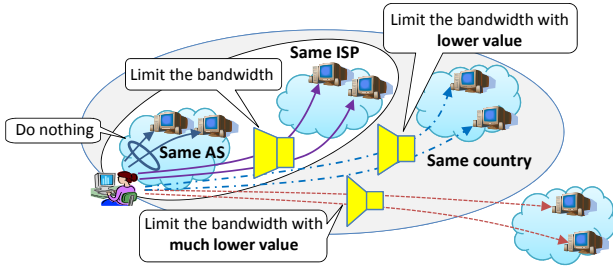


Fig. 2: The concept of hierarchical bandwidth limitation scheme.

where B is a bandwidth unit, and ε_1 is a tiny constant to ensure the denominator of the fraction never come to zero.

From above equations, we defined the allocated bandwidth of a candidate peer based on not only the physical distance but also the number of peers in the same area as the querying peer. This enables our method to realize the hierarchy of localization. For instance, if no candidate peer exists in the same AS or ISP, i.e., $n_1 = n_2 = 0$, the first two exponential functions in Eq. (2) will come to zero, the logical distance will therefore depend only on the country information. In the worst case, if no candidate peer exists in the same country as the querying peer, $n_1 = n_2 = n_3 = 0$, the logical distance will be almost zero; the limited bandwidth for every peer in Eq. (6) will go to $+\infty$, which means that no bandwidth limitation is applied. Therefore, the proposed method will not affect the performance of P2P applications even when no local peer exists.

C. Proposed router architecture

We introduce a router-aided approach to implement the proposed method independently of the P2P applications. Figure 3 shows the architecture of the router. Three modules, a traffic classification, location identifier, and bandwidth limitation module, are added into a common router. The traffic classification module classifies the input traffic into P2P or non-P2P traffic. To avoid the degradation of service quality of non-P2P applications, the non-P2P traffic goes directly to the common router function. In the location identifier, the destination IP address of every P2P packet is first examined. The identifier then resolves the location information of the destination by using several IP-to-geographic-location database services. According to this geographical location information, the bandwidth limitation module limits the bandwidth of connection between the querying peer and the candidate peer. The limited bandwidth for each peer is computed according to Eqs. (1) and (6) for the fixed-length bandwidth limitation scheme and the hierarchical bandwidth limitation scheme, respectively.

IV. IMPLEMENTATION OF PROPOSED METHOD

To implement the proposed router, we set up a PC-based router equipped with an Intel Core i7-2600 3.4 GHz CPU, 12 GB of DDR3 memory, and two 1 Gbps Ethernet network interface cards, operated under Linux Ubuntu 12.04 with 3.2.0-29 generic kernel.

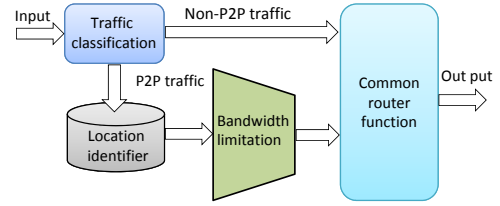


Fig. 3: The proposed router architecture.

In the research field of traffic classification, there are many methods that have been previously proposed. For instance, to block P2P traffic, ISPs usually apply deep packet inspection and session-based classification with 5 tuples (IP addresses, port numbers, and protocol type). In our previous work, we could easily check the peer list format of some P2P streaming applications because the peer list were sent in clear text without any encoding [18]. Therefore, all traffic transferred with the peers existing in the peer list can be recognized as P2P traffic. Recently, an accurate behavioral classification method for P2P traffic, named “Abacus, has been proposed [19]. Abacus relies only on the count of packets and bytes that peers exchange during small fixed-length time windows. Therefore, we can utilize such type of the above methods to implement the traffic classification module in our router. In this study, however, we assume that such the classification module is beyond the scope of this paper, and thus focus only on the implementation of bandwidth limitation module to verify the effectiveness of traffic localization in a real network.

The bandwidth limitation module is implemented in the following main steps:

- *Packet monitoring*: we use `libpcap`, a well-known packet capture library to examine all packets going through the router [20]. The headers of the packets are checked to read their source and destination IP addresses.
- *IP-to-location mapping*: the locations of the obtained IP addresses are then resolved by using IP-to-location services. In this implementation, we use GeoLite database services including GeoLite ASN, GeoLite City, and GeoLite Country, which are free IP geolocation databases created by MaxMind [21].
- *Computation of logical distance and limited bandwidth value*: The limited bandwidth for each candidate peer is computed according to Eqs. (1) and (6) for the fixed-length bandwidth limitation scheme and the hierarchical bandwidth limitation scheme, respectively.
- *Bandwidth limitation*: for the bandwidth limitation, we utilize `dummynet`, a flexible tool for simulating packet filtering, bandwidth management, packet delay, and packet loss [22]. By changing the configuration of `ipfw` firewall, a user interface provided by `dummynet`, we can easily setup many pipes between sender and receiver peers. All the packets will be carried in these pipes. Each pipe can be configured with a different bandwidth value computed from the previous step.

For the fixed-length bandwidth limitation scheme, the value of limited bandwidth is constant for all foreign peers. The implementation is therefore very simple as shown in algorithm

Algorithm 1: Fixed-length bandwidth limitation scheme:
configure the bandwidth for a new peer

Data: New packet, List of connected IP addresses: ip_list
Result: Configure the bandwidth for a candidate peer

```

1 while TRUE do
2   packet  $\leftarrow$  read_new_packet();
3   ip  $\leftarrow$  check_header(packet);
4   if ip is new then
5     country_code  $\leftarrow$  resolve_location(ip);
6     if country_code  $\neq$  "JP" then
7       bw  $\leftarrow$  C;
8       call_dummysnet_for_limiting_bandwidth(ip, bw);
9     else
10      do_nothing;
11   ip_list  $\leftarrow$  add_new_ip_to_list(ip);
12 else
13   do_nothing;
```

Algorithm 2: Hierarchical bandwidth limitation scheme:
configure the bandwidth for a new peer

Data: New packet
Result: Configure the bandwidth for a new peer

```

1 while TRUE do
2   packet  $\leftarrow$  read_new_packet();
3   ip  $\leftarrow$  check_header(packet);
4   if ip is new then
5     (as, isp, country, lat, lon)  $\leftarrow$  resolve_location(ip);
6     (n1, n2, n3)  $\leftarrow$  update_no_peers_same_area(as, isp, country);
7     logical_distance  $\leftarrow$  compute_logical_distance(as, isp, country, lat, lon, n1, n2, n3);
8     bw  $\leftarrow$  compute_limited_bandwidth(logical_distance);
9     call_dummysnet_for_limiting_bandwidth(ip, bw);
10    ip_list  $\leftarrow$  add_new_ip_to_list(ip);
11  else
12    do_nothing;
```

1. For every new peer coming to the router, we simply check its country information and apply bandwidth limitation if the peer does not come from Japan.

For the hierarchical bandwidth limitation scheme, the value of limited bandwidth depends on the numbers of peers in the same area as the querying peer. Since these numbers may be changed when a new peer comes, the limited bandwidth values of all connected peers should be recomputed again many times. This causes high CPU usage and affects other processes of the router. In addition, the bandwidth limitation strategy might not be effective in traffic localization if we change the configuration too often. Therefore, our solution is to compute the limited bandwidth for the new peer in real time and to recalculate the limited bandwidth for all the connected peers every one minute. This avoids the high load on the router's CPU, and ensures a regular updating of the bandwidth value for all connections. Algorithms 2 and 3 show pseudo codes of bandwidth configuration for a new peer and bandwidth reconfiguration for a list of connected peers, respectively.

V. EXPERIMENTAL RESULTS

A. Experimental setup

In this setup, the proposed router is placed as a subnet gateway router as shown in Fig. 4. We performed experiments

Algorithm 3: Hierarchical bandwidth limitation scheme:
reconfigure the bandwidth for all connected peers

Data: List of connected IP addresses: ip_list
Result: Reconfigure the bandwidth for all connected peers

```

1 call_dummysnet_for_flushing_all_old_configurations();
2 (n1, n2, n3)  $\leftarrow$  count_no_peers_same_area(ip_list);
3 for i = 1 to count(ip_list) do
4   (as, isp, country, lat, lon)  $\leftarrow$  get_location(ip_list[i]);
5   logical_distance  $\leftarrow$  compute_logical_distance(as, isp, country, lat, lon, n1, n2, n3);
6   bw  $\leftarrow$  compute_limited_bandwidth(logical_distance);
7   call_dummysnet_for_limiting_bandwidth(ip, bw);
```

using P2PTV applications because of their popularity. Two types of P2PTV applications are selected: SopCast version 3.5.0 for performing video live streaming and PPStream version 3.2.0.1067 for performing video-on-demand service. These applications did not consider peer locality, as reported in several previous studies [23], [24]. We set each application to run one-by-one on the measurement hosts. On SopCast we played a live Chinese channel, CCTV-2. On PPStream, an on-demand drama popular in Japan was selected for the experiment. The average bit rates of these two video streams were 800kbps and 705kbps, respectively. Since we also wanted to check the possibility that a measurement host downloading the video data from the very neighbor peer inside our laboratory, we always run each P2P application on two measurement hosts simultaneously, as host 1 and host 2. All the experiments were conducted in September 2013 in our laboratory. The location information of measurement hosts in detail is as follows:

- AS number: AS4713
- ISP: NTT Communications Corp.
- Country: Japan.

We utilize Wireshark [25], a well-known packet sniffer application, to generate statistical information of traffic on the measurement hosts. Since we skip the implementation of the traffic classification module, only P2P applications and Wireshark are permitted to run on the measurement hosts.

The values of the parameters in the equations were chosen as follows: $C = 800$, $\varepsilon = 0.1$, $\theta_1 = \theta_2 = 1000$, $\theta_3 = 2000$, $\varepsilon_1 = 1$, and $B = 2000000$.

B. Criteria of Evaluation

To evaluate the effectiveness of the proposed method, we compared the results of three different schemes: (1) random and/or RTT-based peer-selection scheme, i.e., the original behavior of P2PTV applications; (2) fixed-length bandwidth

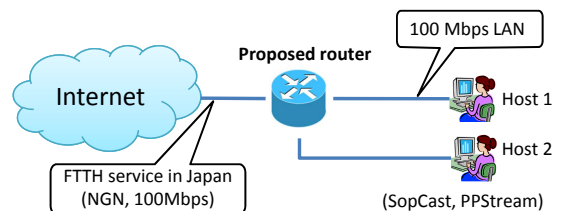


Fig. 4: The proposed router architecture.

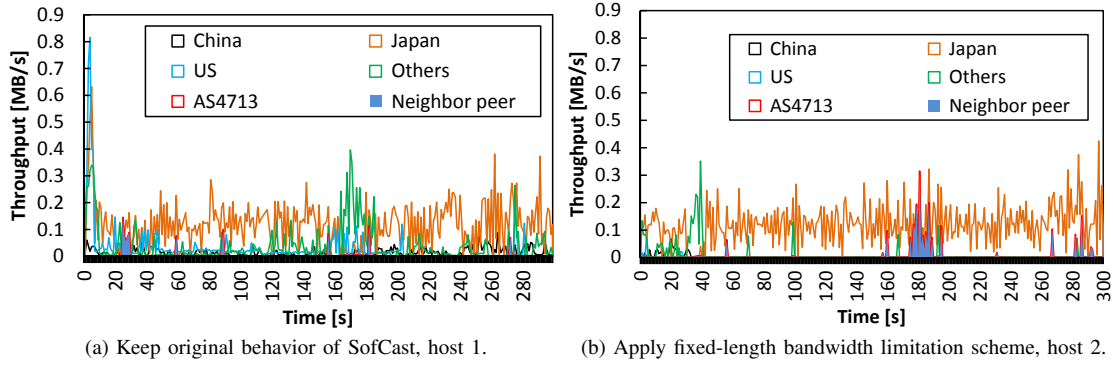


Fig. 5: Temporal changes of throughput when simultaneously keeping original behavior of SopCast on the measurement host 1 and applying the fixed-length bandwidth limitation scheme on the measurement host 2.

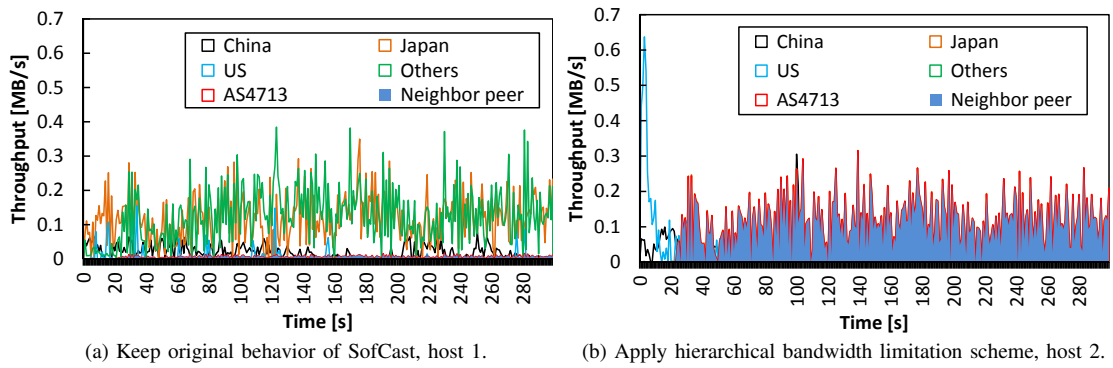


Fig. 6: Temporal changes of throughput when simultaneously keeping original behavior of SopCast on the measurement host 1 and applying the hierarchical bandwidth limitation scheme on the measurement host 2.

limitation scheme, in which the bandwidth of all the connections to foreign peers were limited at 800kbps maximum. We chose 800kbps as a limited value because 800kbps is approximate equal to the average bit rates of the two video streams of SopCast and PPStream; (3) hierarchical bandwidth limitation scheme.

We compared the results of three schemes from two viewpoints: the traffic locality and the QoS. From the former viewpoint, we measured the volume of downloaded data and the number of neighbor peers, and reported their ratios by regions as evaluation indexes. For each scheme, we ran each P2P application three times, with 300 seconds each time. The means of evaluation indexes were calculated as final results.

From the latter viewpoint, QoS, we evaluated the quality performance of SopCast and PPStream. Since SopCast is a live streaming application, we measured the average waiting time of users. The waiting time is the time that users have to wait for the application to buffer enough data for starting playing. Therefore, the waiting time reflects the down load speed, and thus can be used as a metric for evaluating the application performance. On PPStream, because we ran an on-demand video, we measured the size of cached file buffered by PPStream within 300 seconds of the measurement.

C. Results with SopCast

First, we present the results obtained with SopCast. Figure 5 shows an example of temporal changes of throughput when keeping original behavior of SopCast on the measurement host 1 and applying the fixed-length bandwidth limitation scheme on the measurement host 2. In case of no limitation, traffic measured on host 1 comes from many countries including China, Japan, the United State and the others. However, host 1 did not recognize and download video data from the very neighbor peer, host 2. In particular, the traffic coming from host 2 is zero as shown in Fig. 5 (a). In case of applying fixed-length bandwidth limitation, most traffic measured on host 2 comes from Japan because SopCast tends to remove connection paths with foreign peers due to a lower bandwidth. However, the traffic coming from the very neighbor peer, host 1, is very small. This is because the scheme does not distinguish the very neighbor peer from the other Japanese peers, SopCast can download video data pieces from the very neighbor peer at one time, and from other Japanese peers at other times when the new peers are better.

Figure 6 shows an example of temporal changes of throughput when keeping original behavior of SopCast on the measurement host 1 and applying the hierarchical bandwidth limitation scheme on the measurement host 2. With the hierarchical scheme, almost all the traffic measured on host

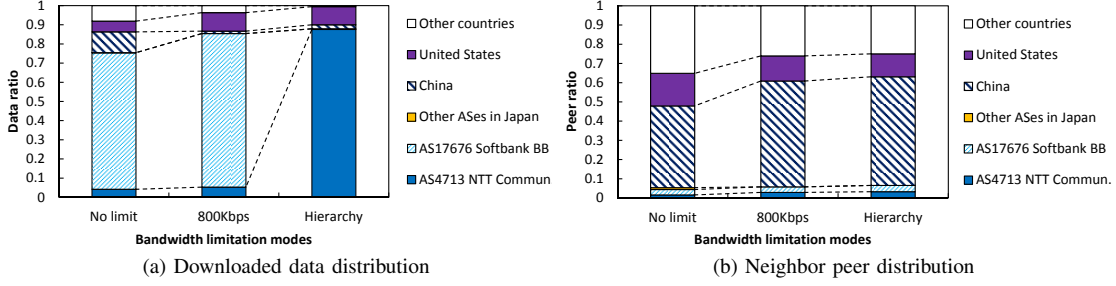


Fig. 7: Downloaded data distributions and neighbor peer distributions for SopCast in three modes of bandwidth limitation.

TABLE I: Average waiting time of SopCast.

Bandwidth limitation modes	Average waiting time [s]
No limit	13.45
Fixed-length (800kbps)	42.50
Hierarchy	14.00

2 is downloaded from the very neighbor peer, host 1, with IP address 192.168.12.32 as shown in Fig. 6 (b). In contrast, at the same time host 1 could not download any video data from its very neighbor peer, host 2. This is because our hierarchical scheme has degraded network performance of inter-AS connections by limiting their bandwidth. Therefore, SopCast tends to preferably download video data pieces from the neighbor peer in the same AS that usually has better performance than other peers, e.g., shorter RTT. The feature of our hierarchical bandwidth limitation scheme that forces a P2P streaming application to download the data from a peer in the same LAN is very significant. To the best of our knowledge, no other research shows the same result to ours.

Figure 7 (a) presents the average downloaded data distributions by three schemes. The vertical axis represents the region-by-region ratios for the downloaded traffic that the measurement host received from other peers. We listed the ratios by ASes/ISPs for the traffic inside Japan, and by countries for the overseas traffic. The information of AS and ISP was grouped together in the results because we had not found any traffic coming from different AS in the same ISP in the experiments. We marked that the traffic coming from outside of AS4713 NTT Communications Corp. as cross-AS/ISP traffic. The cross traffic accounts for 95% of the total traffic in case of no limit, i.e., original behavior of SopCast. This is a very high percent of inter-domain traffic. In case of fixed-length bandwidth limitation scheme, almost all traffic comes from Japan. This indicates that SopCast tends to preferably download data pieces from Japanese peers that have better performance than foreign peers due to bandwidth limitation applied to overseas traffic. However, the cross-AS/ISP traffic is still very high, which accounts for 94% of the total traffic. On the other hand, with the hierarchical bandwidth limitation scheme, such the cross traffic accounts for only 13% of the total traffic. This statistic shows that our hierarchical scheme significantly reduces the cross-AS/ISP traffic.

Figure 7 (b) illustrates the neighbor peer distributions by three schemes, where the vertical axis represents the region-

TABLE II: Average size of cached file buffered by PPStream within 300 seconds.

Bandwidth limitation modes	Size of cached file [MB]
No limit	195
Fixed-length (800kbps)	43
Hierarchy	193

by-region ratios of the number of peers that the measurement host communicated with. Figure 7 (b) indicate that the neighbor peer distributions do not vary much and almost independent of the bandwidth limitation. This can be explained as follows: SopCast first contacts with some peer list servers to obtain a list of available online peers, and then forms an overlay network for exchanging video data pieces with a subset of those peers. Our bandwidth limitation schemes, however, cannot intervene at the step of obtaining the peer list. The neighbor peer distributions are therefore pretty stable. Nevertheless, the application preferably selects closer peers to download data pieces even when very few candidates exist. Our proposal thus successfully realizes traffic localization on SopCast.

Table I shows the average waiting time for SopCast by three schemes. It is easy to see that the fixed-length bandwidth limitation scheme degrades the performance of SopCast. In comparison with the original behavior of SopCast, the waiting time is much longer in case of 800kbps bandwidth limitation. This is because the fixed-length bandwidth limitation scheme always limits the bandwidth of overseas traffic even when very few Japanese peers exist for localizing. In the worst case, no Japanese peer for contact, the waiting time of SopCast will be very long due to bandwidth limitation applied to overseas traffic. In contrast, the waiting time of the hierarchical bandwidth limitation scheme is almost the same as that of the original behavior. These results show the effectiveness of the hierarchical feature. In case of no Japanese peer for contact, no bandwidth limitation is applied as described in previous section. Therefore, we conclude that the hierarchical bandwidth limitation scheme also maintains the quality performance of SopCast.

D. Results with PPStream

Secondly, we present the results obtained with PPStream. The experiments are performed in a similar manner to SopCast case. Figure 8 presents an example of throughput changing

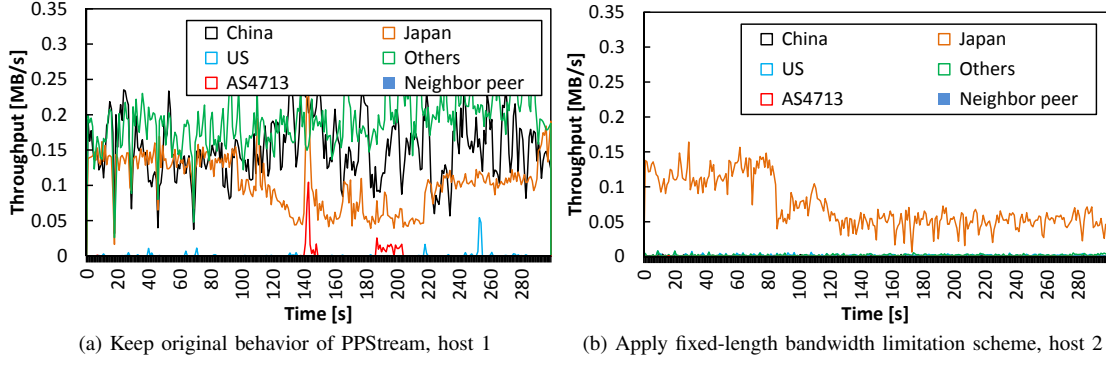


Fig. 8: Temporal changes of throughput when simultaneously keeping original behavior of PPStream on the measurement host 1 and applying the fixed-length bandwidth limitation scheme on the measurement host 2.

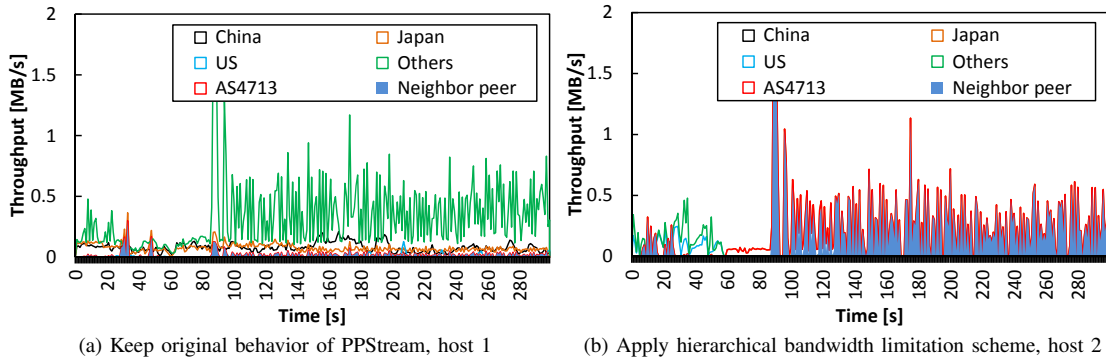


Fig. 9: Temporal changes of throughput when simultaneously keeping original behavior of PPStream on the measurement host 1 and applying the hierarchical bandwidth limitation scheme on the measurement host 2.

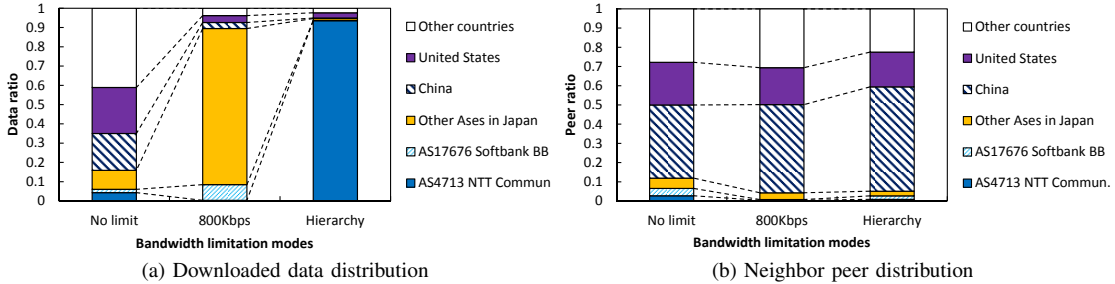


Fig. 10: Downloaded data distributions and neighbor peer distributions for PPStream in three modes of bandwidth limitation.

when simultaneously keeping original behavior of PPStream on the measurement host 1 and applying fixed-length bandwidth limitation scheme on the measurement host 2. The results resemble the SopCast case. In particular, when applying the fixed-length bandwidth limitation, almost all the traffic measured on host 2 comes from Japan. This feature proves the success of bandwidth limitation scheme in P2P traffic localization. However, both hosts could not recognize the very neighbor peer to download video data pieces. In contrast, Fig. 9 indicates that in case of applying the hierarchical bandwidth limitation on host 2 and keeping original behavior of PPStream on host 1, almost all the traffic comes from the very neighbor peer, host 1. Simultaneously, host 1 did not download any

video data from its very neighbor peer, host 2.

Figure 10 shows the downloaded data distributions and the neighbor peer distributions by three schemes. The results indicate that even though the neighbor peer distributions are fairly steady, the amount of data received from Japan increases dramatically in case of applying bandwidth limitation method. Furthermore, the amount of the cross-AS/IP traffic decreases significantly when applying the hierarchical bandwidth limitation scheme. As shown in Fig. 10 (a), the cross-AS/ISP traffic accounts for 95%, 99%, and 6% of the total traffic in case of no limit, fixed-length bandwidth limitation, and hierarchical bandwidth limitation scheme, respectively.

Table II presents the average size of cached file for PP-

Stream within five minutes by three schemes. Similar to SopCast case, the fixed-length bandwidth limitation scheme also degrades the performance of PPStream. In particular, the average cached file size in case of fixed-length scheme is 43MB, much smaller than that of original behavior of PPStream, 195MB. On the other hand, the cached file size of the hierarchical bandwidth limitation scheme is almost the same as that of no limitation case. Based on the very similarity in results of PPStream and Sop-Cast, we believe that the communication protocols of these two applications are probably very similar.

VI. CONCLUSION

In summary, this paper provides the following meaningful contributions to the field of P2P traffic localization: (1) we proposed two different schemes based on bandwidth limitation, to solve the problem on network layer; (2) with the hierarchical scheme, the traffic can be localized hierarchically with multiple levels including AS level, ISP level, and country level; (3) our proposals requires neither modification of existing application software, nor dedicated server, nor collaboration between ISPs and P2P users. The experiment measurements indicate that the fixed-length bandwidth limitation successfully realized traffic localization by the suppression of the connection paths with the foreign peers. Moreover, our hierarchical bandwidth limitation scheme significantly reduces the cross AS/ISP traffic. In particular, the cross-AS/ISP traffic decreases by 82% for SopCast and 91% for PPStream, in comparison to original behavior of these two applications.

Several future challenges remain. First, we only measured the waiting time as a QoS evaluation metric. In the future, we will investigate the QoS with many other factors when applying the bandwidth limitation. Second, the effectiveness of our proposed router in a real network might be influenced much by the accuracy of the traffic classification module. Therefore, we are also planning to consider deeply the traffic classification module to complete our router-aided approach.

ACKNOWLEDGMENT

This study was partly supported by a Grant-in-Aid for Young Scientists (B) No. 23760344 from the Japan Society for the Promotion of Science (JSPS).

REFERENCES

- [1] R. Dunaytsev, D. Moltchanov, Y. Koucheryavy, O. Strandberg, and H. Flinck, "A survey of p2p traffic management approaches: best practices and future directions," *Internet Engineering*, vol. 5, no. 1, pp. 318–330, June 2012.
- [2] T. Karagiannis, P. Rodriguez, and K. Papagiannaki, "Should internet service providers fear peer-assisted content distribution?" in *Proc. Internet Management Conf. (IMC 2005)*, Oct. 2005, pp. 63–76.
- [3] L. Plissonneau, J. Costeux, and P. Brown, "Detailed analysis of edonkey transfers on adsl," in *Proc. 2nd Conf. Next Generation Internet Design and Engineering (NGI '06)*, April 2006, pp. 256–262.
- [4] V. Aggarwal, A. Feldmann, and C. Scheideler, "Can isps and p2p users cooperate for improved performance?" *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 29–40, July 2007.
- [5] H. Xie, Y. Yang, A. Krishnamurthy, Y. Liu, and A. Silberschatz, "P4p: provider portal for applications," in *Proc. ACM SIGCOMM 2008*, Aug. 2008, pp. 351–362.

- [6] J. Seedorf, S. Kiesel, and M. Stiernerling, "Traffic localization for p2p-applications: the alto approach," in *Proc. IEEE Int. Conf. Peer-to-Peer Comput. (P2P2009)*, Sept. 2009, pp. 171–177.
- [7] R. Alimi, R. Penno, and Y. Yang, "Alto protocol," in *Internet draft, draft-ietf-alto-protocol-10.txt*, Oct. 2011.
- [8] D. Choffnes and F. Bustamante, "Taming the torrent - a practical approach to reducin cross-isp traffic in peer-to-peer systems," in *Proc. ACM SIGCOMM2008*, Aug. 2008, pp. 363–374.
- [9] R. Bindal, P. Cao, W. Chan, J. Medved, G. Suwala, T. Bates, and A. Zhang, "Improving traffic locality in bittorrent via biased neighbor selection," in *Proc. IEEE Int. Conf. Distributed Comput. Syst. (ICDCS2006)*, July 2006.
- [10] H.-Y. Lee and A. Nakao, "Isp-driven delay insertion for p2p traffic localization," *IEICE Trans. Commun.*, vol. E96-B, no. 1, pp. 40–47, Jan. 2013.
- [11] —, "A feasibility study of p2p traffic localization through network delay insertion," *IEICE Trans. Commun.*, vol. E95-B, no. 11, pp. 3464–3471, Nov. 2012.
- [12] T. Miyoshi, Y. Shinozaki, and O. Fourmaux, "A p2p traffic localization method with additional delay insertion," in *Proc. 4th Int. Conf. Intelligent Networking and Collaborative Syst. (INCoS2012)*, Sept. 2012, pp. 148–154.
- [13] Cisco System, Inc. "Cisco visual networking index: forecast and methodology, 2011-2016," White paper, May 2012.
- [14] PPTV. [Online]. Available: <http://www.pptv.com/>.
- [15] PPStream. [Online]. Available: <http://www.pps.tv/>.
- [16] SopCast. [Online]. Available: <http://www.sopcast.com/>.
- [17] Zattoo. [Online]. Available: <http://zattoo.com/>.
- [18] H. Hoang-Van, T. Miyoshi, and O. Fourmaux, "P2ptv traffic localization by deep packet inspection," in *Proc. IEEE/ACIS-SNPD 2013 (Honolulu)*, July 2013, pp. 375–380.
- [19] S. Valenti and D. Rossi, "Fine-grained behavioral classification in the core: the issue of flow sampling," in *Proc. 7th Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC2011)*, July 2011, pp. 1028–1032.
- [20] Tcpdump and libpcap pulbic repository. [Online]. Available: <http://tcpdump.org/>.
- [21] MaxMind and GeoIP, IP address location technology. [Online]. Available: <http://www.maxmind.com/app/ip-location/>.
- [22] Dummynet. [Online]. Available: <http://info.iet.unipi.it/~luigi/dummynet/>.
- [23] X. Su and L. Chang, "A measurement study of ppstream," in *3rd Int. Conf. Commun. and Networking in China (ChinaCom 2008)*, Aug. 2008, pp. 1162–1166.
- [24] A. Horvath, M. Telek, D. Rossi, P. Veglia, D. Ciullo, M. Garcia, E. Leonardi, and M. Mellia, "Dissecting pplive, sopcast, tvants," NAPA-WINE project, Tech. Rep., 2009.
- [25] Wireshark. [Online]. Available: <http://www.wireshark.org/>.



Hiep Hoang-Van received the B.E. and M.S. degrees in computer engineering and communication from Hanoi University of Science and Technology in 2007 and 2011, respectively. Currently, he is doing his research as a doctoral student at Graduate School of Engineering and Science, Shibaura Institute of Technology, Japan. His research interests include multimedia communication technologies, P2P systems, P2P traffic engineering. He is a student member of IEICE.



Takumi Miyoshi received the B.Eng., M.Eng., and Ph.D. degrees in electronic engineering from the University of Tokyo, Japan, in 1994, 1996, and 1999, respectively. He was a visiting associate from 1994 to 1996 and an Internet technical staff from 1996 to 1997 at the Institute for Monetary and Economic Studies, Bank of Japan. He was also a research associate at Global Information and Telecommunication Institute, Waseda University, from 1999 to 2001, and a research fellow at Telecommunications Advancement Organization of Japan from 1998 to

2003. He is presently a professor at Department of Electronic Information Systems, College of Systems Engineering and Science, Shibaura Institute of Technology, Saitama, Japan. He was a visiting scholar at Laboratoire d'Informatique de Paris 6 (LIP6), UPMC Sorbonne Universités (Paris 06), Paris, France, from 2010 to 2011. His research interests include multimedia communication technologies, mobile ad hoc and sensor networks, and online learning systems. He received the IEICE Young Investigators Award in 2004, the IEICE Network System Research Award in 2010, the IEICE Information Network Research Award in 2001, 2004, and 2006, the IEICE Communications Society Distinguished Contributions Award in 2006, 2007, 2009, and 2010, and Ericsson Young Scientist Award in 2002. He is also a member of IEEE.



Olivier Fourmaux is an associate professor at UPMC Sorbonne Universités (Paris 06), France, since 2003. Before, he was an assistant professor at Institut Galilée, Université Paris 13, France. He received his Ph.D. degree in computer networking in 1998 and his M.Sc. degree in computer systems in 1995, both from UPMC. His research interests are content delivery networks, P2P networks, active networks and multimedia in high-speed networks. He is a member of the Network and Performance group of the LIP6 Laboratory (CNRS-UPMC). He

is also a member of IEEE.