# An Automated Framework for the Management of P2P Traffic in ISP Infrastructures

Pedro Sousa

**Abstract** Peer-to-Peer (P2P) is nowadays a widely used paradigm underpinning the deployment of several Internet services and applications. However, the management of P2P traffic aggregates is not an easy task for Internet Service Providers (ISPs). In this perspective, and considering an expectable proliferation in the use of such applications, future networks require the development of smart mechanisms fostering an easier coexistence between P2P applications and ISP infrastructures. This paper aims to contribute for such research efforts presenting a framework incorporating useful mechanisms to be activated by network administrators, being also able to operate as an automated management tool dealing with P2P traffic aggregates.

## 1 Introduction

P2P overlay networks [1] are becoming omnipresent in current networking infrastructures and it is expected that many future Internet applications may increasingly rely on this network communication paradigm. However, some P2P applications, as BitTorrent [2], are responsible by a relevant portion of the Internet traffic [5] and their behavior is many times unpredictable, generating high volumes of traffic traversing network infrastructures and leading to coexistence problems with ISPs. As a consequence, several efforts have been made in order to attain ISP-friendly P2P solutions (e.g. [8, 9]). Aligned with such efforts there is also the need for efficient and automated management mechanisms allowing ISP administrators to better deal with P2P traffic aggregates in their infrastructures, in place of being only restricted to use traditional bandwidth throttling mechanisms [6].

In this context, this work presents the rationale of an automated framework able to contribute for a better coexistence between ISPs and P2P applications. The frame-

Pedro Sousa
Centro Algoritmi/Department of Informatics, University of Minho, Braga, Portugal
e-mail: pns@di.uminho.pt

work is sustained by a BitTorrent-like collaborative P2P system integrating configurable P2P trackers also with the ability to exchange valuable information with the ISP level (as also proposed by other works, e.g [7]). Based on the devised framework some illustrative capabilities are described, focusing on some methods that can be useful from the ISP point of view, namely: the capability to estimate the traffic impact that a given P2P swarm will have on the ISP infrastructure; the ISP ability to divert P2P traffic from specific network components of the network topology; the inclusion of mechanisms allowing for P2P service quality differentiation. With the proposed solution, network administrators may explicitly trigger the described mechanisms whenever required, or use the framework as an automated tool to implement specific policies controlling the P2P traffic aggregates in the ISP domain.

Section 2 presents the rationale of the proposed framework and Section 3 explains some of the supported methods. The simulation platform is described in Section 4 along with illustrative results. Finally, Section 5 concludes the paper.

## 2 Framework Architecture

Figure 1 presents the main components of the devised framework: *i)* illustrative network management and optimization tasks usually required to manage and improve the ISP infrastructures; *ii)* the ISP infrastructure integrating several links and routers, some of which providing access to ISP end-users/customers; *iii)* the P2P tracker internal components. The framework assumes the scenario where P2P applications and the ISP assume collaborative behaviors. Furthermore, the framework assumes the specific case of BitTorrent [2, 10] like applications, here with the tracker being the unique entity able to provide peering information, returning for this purpose a random sample of peers participating in the swarm to contacting peers. As depicted in Figure 1 the ability to manage P2P traffic aggregates in a given infrastructure has also some relevance for other management/optimization tasks (e.g. traffic matrices estimation [3], routing optimization [4], QoS provisioning, etc.). The proposed framework assumes the existence of a P2P traffic management module (which may assume an automated behavior or be directly controlled by an administrator) able to interact with a configurable P2P tracker(s) (e.g. [11]) controlling the P2P swarm(s) behavior. The internal modules of the configurable P2P tracker are also depicted in Figure 1, where several mechanisms are available to be activated/programmed by the P2P traffic management module (using the tracker management interface).

The devised framework assumes a collaborative perspective between the ISP and P2P levels. This is materialized by the existence of network level ISP collaborative services able to interact with the P2P tracker (using the tracker external interface), as depicted in Figure 1. Using this interface the P2P tracker is able to access several network level information useful in the context of some specific tracker configurations (e.g. network topology, routing paths, network location of specific peers, etc.). As a reward for assuming a collaborative perspective the traffic generated by P2P applications using the proposed framework are positively discriminated by the ISP.

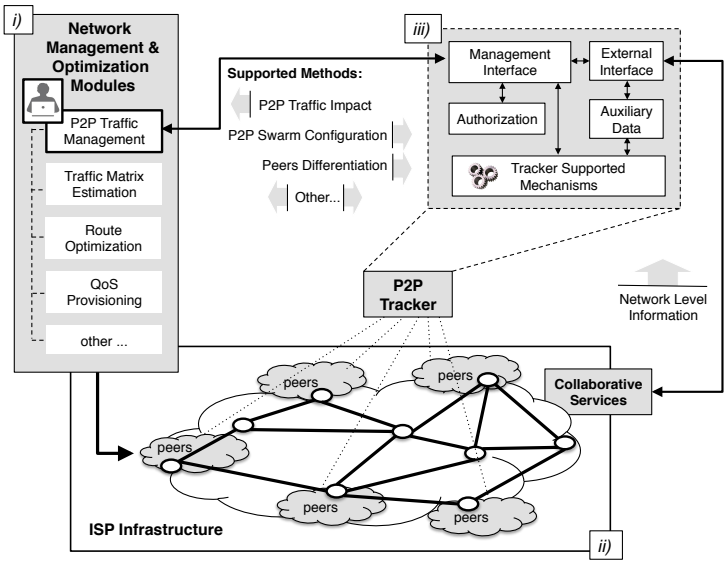


**Fig. 1** High level description of the P2P management framework and associated components.

## 3 Examples of Methods Supported by the P2P Tracker

### *3.1 P2P Impact Estimation*

This mechanism allows the P2P tracker to inform the P2P Traffic Management module (or the administrator) about the traffic impact that a given pre-scheduled P2P swarm, involving a considerable number of peers, will have in the network links of the ISP. Based on this feedback, and depending on the particular objectives in place, the ISP is able to influence the P2P swarm composition in order to protect specific elements from the underlying infrastructure (method described in section 3.2).

The behavior of a P2P system as the assumed here is influenced by a large number of factors, as network level factors (e.g. network topology, peers locations, network paths, etc.) and data transfer protocol level factors (e.g. rules used by peers to exchange data pieces, etc). Such large number of factors affecting the P2P overlay, along with the fact that some of those are extremely hard to foresee, make very difficult to define a highly accurate model to estimate the P2P traffic impact. The presented method centers the estimation efforts on the particular case of large BitTorrent P2P swarms and focus on specific network level factors that have major influence on the P2P traffic distribution. To evaluate the P2P traffic impact on the network links the P2P tracker models the network ISP infrastructure as a graph $G = (N, L)$. Furthermore, the tracker will receive from ISP level collaborating services other associated information, such as: network peers location (peers are located on end-users areas), network topology, routing information, etc.. In a simpli-

**Table 1** Syntax of the symbols used to compute the P2P link impact values

| Symbols | Description |
|---|---|
| $G = (N, L)$ | Graph expressing a network infrastructure (e.g. an ISP) |
| $L$ | Set of network links of the ISP |
| $N$ | Set of network nodes/routers of the ISP |
| $A$ | Set of end-user areas where peers are located (each area is denoted by the corresponding network router, $a$, with $a \in A$ and $A \subseteq N$) |
| $paths_{i,j}$ | Number of shortest paths between end-user areas $i$ and $j$ |
| $paths_{i,j}(l)$ | Number of shortest paths between end-user areas $i$ and $j$ that include link $l$ |
| $lif_{i,j}(l)$ | Link inclusion factor for link $l$ considering areas $i, j$, with $lif_{i,j}(l) = \frac{paths_{i,j}(l)}{paths_{i,j}}$ |
| $w_{i,j}$ | Ratio between the number of peers involved in possible peering adjacencies involving areas $i, j$ and the number of peers involved in possible adjacencies involving all areas |
| $p_{i \leftarrow j}$ | Factor denoting how close are areas $j$ and $i$, with $p_{i \leftarrow j} \in [0,1]$ and $\sum_{j \in A, j \neq i} p_{i \leftarrow j} = 1$ |

fied perspective, the model extends and adapts to this P2P approach the concept of betweenness centrality that is one of several graph measures [12, 13]. The model integrates several factors used to estimate the P2P traffic impact in the network links (see Table 1 for a detailed description of the used mathematical symbols): *i)* a link inclusion factor, $lif_{i,j}(l) \in [0,1]$, is evaluated for each link $l \in L$ considering all the available end-user areas pairs. If all the available shortest paths between areas $i, j$ include link $l$ then $lif_{i,j}(l) = 1$; *ii)* a weighting factor, $w_{i,j}$, dealing with unbalanced distribution of peers in the network, increasing the importance of shortest paths connecting areas involving higher number of peers; *iii)* a preference value, $p_{i \leftarrow j}$, favoring near end-user areas pairs, as BitTorrent peers often have a higher probability to establish peering adjacencies with nearest peers in the network favoring TCP connections with lower RTTs. Equation 1 presents the devised normalized P2P impact metric ($I_{P2P}$) for each link $l$ (which assigns impact values in the interval $[0,1]$). This method is used by the tracker to inform the P2P Traffic Management module (of Figure 1) about the estimated impact, where links that are assigned with higher $I_{P2P}(l)$ values are expected to be traversed by higher volumes of P2P traffic.

$$I_{P2P}(l) = \sum_{i,j \in A,\ i \neq j} [(|A| - 1) \cdot p_{i \leftarrow j}] \cdot lif_{i,j}(l) \cdot w_{i,j} \quad l \in L \tag{1}$$

## *3.2 ISP-controlled P2P Swarms*

The framework also allows the ISP to influence the P2P swarms operation. The methods might be triggered by the administrator or integrate an automated approach programmed in the P2P Traffic Management module, e.g. allowing to react to the traffic impact values provided by the tracker or other events. Figure 2 depicts some supported methods: *link/router protection,* the tracker is informed that a given network link/router equipment should be protected from P2P traffic; *overlay minimization,* the tracker should minimize the number of routers/links traversed by P2P traf-

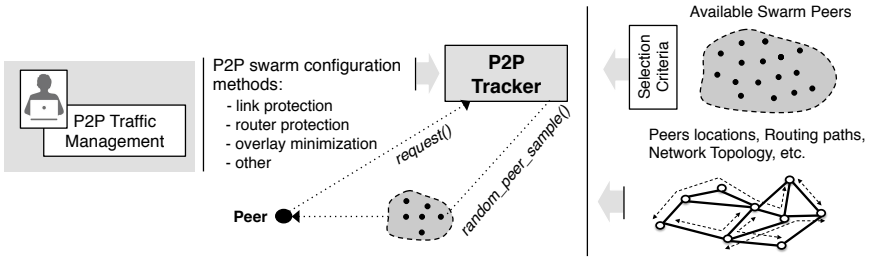


**Fig. 2** High level description of methods of the framework allowing ISP-controlled P2P swarms.

fic. As depicted in Figure 2, the P2P tracker computes the best peer sample to be returned to a given peer based on: the activated method imposing a given selection criteria, the contacting peer id, the available peers of a swarm and the collaborative information provided by the network level. Algorithm 1 presents a pseudo-code of the *router protection* method that can be activated by the P2P Traffic Management module or the administrator. The algorithm assumes a $P_s$ set with all end-user areas pairs having swarm $s$ peers (line 2). Each pair $(a_i, a_j)$ indicates that peers from area $i$ may receive peer samples with peers from area $j$. Next, the set $J$ is defined to contain all links that are connected the router $n$ that the ISP wants to protect (line 3). For each link in $J$ an auxiliary set $Z$ is defined containing area pairs connected by network paths traversing such link (i.e. $lif_{i,j}(l) > 0$, line 5). Next, it is verified if each area pair of $Z$ can be removed from $P_s$ in oder to avoid that such P2P traffic aggregates between the areas traverses router $n$. The pair $(a_i, a_j)$ is only removed (line 8) if the swarm does not get partitioned, i.e. possible connections established between peers of areas $i$ and $j$ are not necessary to guarantee that all peers of the swarm have access to all the pieces upload by the seeds of the swarm. After all the iterations, Algorithm 1 computes the allowed peering adjacencies that can be formed between swarm $s$ peers, expressed by the $P_s$ set. If none of Figure 2 methods is triggered the $P_s$ set will contain all the available area pairs. Thus, when contacted by a given peer the tracker returns a random sample ($random\_peer\_sample()$ in Figure 2) selected from all the available peers not violating the restrictions expressed by $P_s$ set.

## *3.3 Peers Differentiation Strategies*

This section addresses the framework capabilities in order to attain the differentiation of the P2P service offered to the peers. The objective is to enforce the ISP ability to benefit or penalize a given set of peers participating in a specific P2P swarm.

In this context, two method are defined in the framework allowing that the P2P tracker benefits or penalizes a given set of peers of a particular swarm (*penalize_peers()* and *benefit_peers()*, respectively). These methods are able to be used in a wide set of scenarios. As merely illustrative examples, the ISP may explicitly

**Algorithm 1** *router_protection (swarm s, router n, data info)*

1: {$s$: swarm identification; $n$: protected router; *info*: auxiliary data provided by the network}
2: $P_s \leftarrow$ Set with all $(a_i, a_j)$ area pairs having peers from swarm $s$, $a_i, a_j \in A$
3: $J \leftarrow$ Set with all links $l \in L$ that are connect to router $n \in N$
4: **for all** $l \in J$ **do**
5: $Z \leftarrow$ decreasingly ordered subset of $P_s$ with all $(a_i, a_j)$ area pairs having $lif_{i,j}(l) > 0$ {$Z$ is a $w_{i,j} * p_{i \leftarrow j}$ ordered set}
6: **for all** $(a_i, a_j) \in Z$ **do**
7: **if** $swarm\_partitioned(s, P_s \setminus \{(a_i, a_j)\}) = FALSE$ **then**
8: $P_s \leftarrow P_s \setminus \{(a_i, a_j)\}$
9: **end if**
10: **end for**
11: **end for**
12: $update\_allowed\_pairs(s, P_s)$

**Algorithm 2** *penalize_peers(peer p, swarm s)*

1: **if** $action(p, s) == PENALIZE$ **then**
2: **if** first_request($p$, $s$) **or** (current_timer() - last_request_timer($p$, $s$)) $\geq time\_limit$) **then**
3: $peer\_sample \leftarrow$ reduced_peer_sample($s$, $peer\_limit$)
4: **else**
5: $peer\_sample \leftarrow$ null
6: **end if**
7: last_request_timer($p$, $s$) $\leftarrow$ current_timer()
8: **else**
9: $peer\_sample \leftarrow$ random_peer_sample($s$)
10: **end if**
11: update_swarm_info($p$, $s$)
12: return($peer\_sample$)

request the P2P tracker to activate such penalizing methods to punish peers which P2P behavior is contributing to the degradation of the network service quality or, alternatively, benefit specific peers of the P2P swarm as a reward mechanism for their past behavior. Independently of their particular use, the methods might be activated on-the-fly by the network administrator or integrate an automated approach where the P2P Traffic Management module of Figure 1 is programmed to automatically activate such differentiation strategies in the tracker when a given event occur (a specific network condition event, a specific time period during the day, etc.).

Algorithms 2 and 3 present the pseudo-code of the *penalize_peers()* and *benefit_peers()* methods implemented at the tracker. As illustrated in Algorithm 2, the *penalize_peers()* method will firstly verify if the contacting peer belongs to the set of peers that should be penalized. In this case, the adopted strategy is to return to such peers a peer sample with a reduced number of peers (defined by *peer_limit*) and that can only be renewed after a given time (defined by *time_limit*) as observed in lines 2,3 of the algorithm. As consequence, such peers will be limited in the aim of discovering other peers in the swarm, thus experiencing lower service quality levels comparatively to non penalized peers receiving normal samples (line 9).

**Algorithm 3** *benefit_peers(peer p, swarm s)*

```
1: if action(p,s) == BENEFIT then
2:     peer_sample ← privileged_peer_sample(s)
3:     peer_sample ← add_additional_incentives(peer_sample, decision_rule)
4: else
5:     peer_sample ← random_peer_sample(s)
6:     peer_sample ← exclude_privileged_peers(peer_sample)
7: end if
8: update_swarm_info(p, s)
9: return(peer_sample)
```

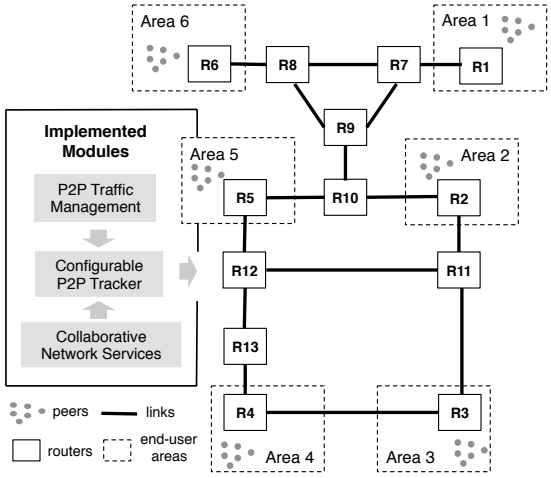


**Fig. 3** Modules implemented in ns-2 and a topology with six end-users areas integrating 300 peers. P2P swarm exchanges a 50MB file with chunks of 256 KB. Peers have upload/download capacities of 1 and 8 Mbps and propagation delays of access links vary within [1, 50]ms. The collaborative scenario assumes 50 Mbps of ISP links reserved for P2P traffic, with propagation delays two times higher than end users access links. By default, the peer sample returned by the tracker has 25 peer contacts.

Algorithm 3 presents the pseudo-code of a tracker strategy benefiting some peers of the swarm. Here, benefited peers will form a privileged sub-swarm that will receive a given incentive which is controlled by the parameter *decision_rule* (lines 2, 3). The other peers will form a normal swarm with no access to such privileges neither to the peers included in the privileged sub-swarm (lines 5, 6). In Section 4 experiments the decision rule for the privileged sub-swarm is to include in the peer sample two seeds with high upload capacity that are hidden from unprivileged peers.

## 4 Simulation Testbed and Illustrative Results

The main components of the framework were implemented at the ns-2 simulator [14] (Figure 3). In order to present some illustrative results the network topology mentioned in Figure 3 was used integrating 300 peers distributed along six end-user areas that participate in a P2P swarm exchanging a 50MB file. In the presented experiments, one seed is assumed to exist in end-user area 1. The network uses the minimum number of hops as the criteria to compute the network routes.

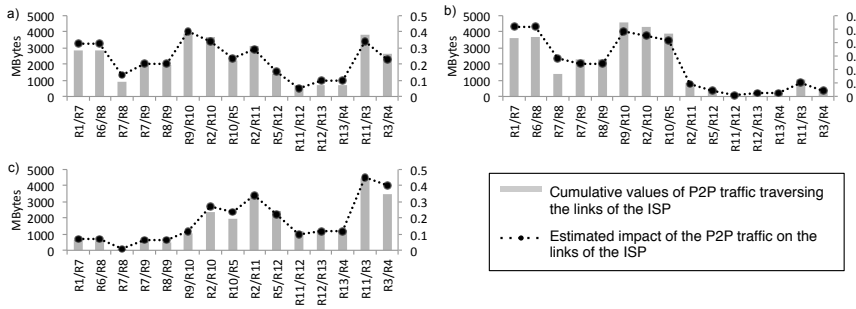


**Fig. 4** P2P traffic vs Estimated $I_{P2P}(l)$ values for each ISP link in scenarios with peers distributions of a) $P_D = (50,50,50,50,50,50)$; b) $P_D = (70,70,10,10,70,70)$; c) $P_D = (10,70,70,70,70,10)$

## *4.1 P2P Impact Estimation*

This example assumes the tracker programmed to inform the P2P Management module about the impact estimation of a given pre-scheduled P2P swarm. Several scenarios involving distinct peers and seeds distributions along the six end-user areas were tested. Due to space constraints only a small set of results are presented, but representative of the mechanism overall performance. Figure 4 presents the comparison between the estimated $I_{P2P}(l)$ metrics[1] and the cumulative traffic values that traversed the ISP links at the end of the simulation time, considering three distinct peers distributions ($P_D$) along the six end-user areas. As observed, the P2P impact metrics follow a similar trend to the traffic aggregates effectively traversing the links, thus provinding a valuable information for network administrators.

## *4.2 ISP-controlled P2P Swarms*

This section presents illustrative results obtained when the P2P Management module of the ISP (or the administrator) instructs the P2P tracker to protect some elements of the topology from P2P traffic (mechanism detailed in Algorithm 1).

Figure 5 a) compares the P2P traffic aggregates that traverses the routers of the ISP when the P2P tracker behaves in the normal configuration mode (white filled bars) and when the tracker is configured by the ISP in order to protect the router *R11* from the topology of Figure 3 (black filled bars). As observed in Figure 5 a) the P2P tracker forced that none of the traffic generated by the P2P swarm traversed the router *R11* of the ISP. A slightly distinct scenario is presented Figure 5 b). Here, the ISP informs the tracker to try to protected router *R9*. As in this specific scenario only one seed is assume to exist in end-user area 1, it is not possible to completely avoid P2P traffic from traversing all *R9* links (otherwise the P2P swarm will become

[1] $p_{i \leftarrow j}$ was set to 0.4 for nearest areas, the remaining areas were assigned with values of 0.15.

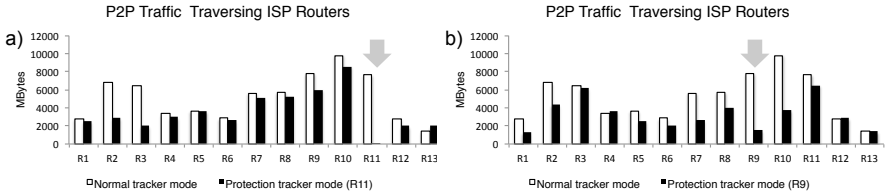


**Fig. 5** P2P traffic traversing each ISP router with the tracker in the normal configuration mode and a) programmed to protect Router 11; b) programmed to protect Router 9.

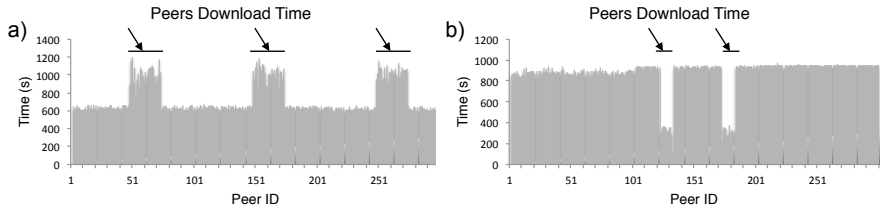


**Fig. 6** Peers download times with tracker programmed to a) penalize $peer_{ids}$ in $(50,75)$, $(150,175)$ and $(250,275)$; b) benefit $peer_{ids}$ within the intervals $(125,135)$ and $(175,185)$.

partitioned). Nevertheless, using the logic of Algorithm 1 the P2P tracker achieves a configuration that allows to substantially reduce the P2P traffic crossing such network element (cumulative amount of P2P traffic traversing *R9* is reduced from 7817 MB to 1575 MB, a decrease of nearly 80% of P2P traffic traversing the equipment).

## *4.3 Peers Differentiation Strategies*

Figure 6 results were obtained during a time period where the P2P Traffic Management module is programmed by the administrator to inform the P2P tracker that when managing new P2P swarms it should penalize/benefit specific network peers. In the first scenario, the tracker penalizes three groups of peers in end-user areas 2, 4 and 6 using the mechanism explained in Algorithm 2, returning a reduced peer sample to those peers (Figure 6 a)). In the second scenario the tracker benefit two specific peer groups from end-user areas 3 and 4 (Figure 6 b)) which form a privileged sub-swarm having access to high upload capacity seeds that are hidden from the other peers of the swarm (using the configuration of Algorithm 3). In both cases there is a clear differentiation in the file download times obtained by distinct peers using the ISP network infrastructure. This confirms that the ISP was able to induce an effective P2P service quality differentiation among the selected peers.

## 5 Conclusions

This paper proposes a P2P management framework based on a BitTorrent-like P2P collaborative system. The solution integrates useful management methods allowing ISPs to better manage P2P traffic aggregates in their network infrastructures. Several illustrative methods were described allowing to automate some important ISP tasks in the context of P2P traffic aggregates management: *i)* the possibility to estimate the traffic impact that a given pre-scheduled P2P swarm will have on the ISP topology; *ii)* the protection of specific network elements from P2P traffic aggregates and *iii)* the capability of the ISP to influence the P2P service quality obtained by the peers.

The devised framework was implemented and tested resorting to simulation. Several examples of the supported methods were presented and corresponding results discussed, clearly corroborating the feasibility of the proposed mechanisms.

**Acknowledgements** This work has been partially supported by FCT - Fundação para a Ciência e Tecnologia Portugal in the scope of the project: UID/CEC/00319/2013.

## References

1. Lua, K., et al.: A survey and comparison of peer-to-peer overlay network schemes. IEEE Communications Surveys & Tutorials, vol 7, Issue 2, pp. 72-93 (2005).
2. Choen, B.: Incentives build robustness in BitTorrent. In Proceedings 1st Workshop on Economics of Peer-to-Peer Systems, Berkeley (June 2003).
3. Tune, P., Roughan, M.: Network-design Sensitivity Analysis. In Proc. of ACM SIGMETRICS 14, 449-461(2014)
4. Pereira, V., Rocha, M., Cortez, P., Rio, M., Sousa, P.: A Framework for Robust Traffic Engineering Using Evolutionary Computation. In G.D. et al. (Ed.), AIMS Conference. Springer, LNCS, vol. 7943, 1-12 (2013)
5. Schulze, H., Mochalski, K.: Internet Study 2007: The Impact of P2P File Sharing, Voice over IP, Skype, Joost, Instant Messaging, One-Click Hosting and Media Streaming such as YouTube on the Internet. Technical Report (2007).
6. Wang, W., Wang, N., Howarth, M., Pavlou, G.: A Dynamic Peer-to-Peer Traffic Limiting Policy for ISP Networks, In Proceedings of NOMS 2010, IEEE/IFIP, pp. 317-324 (2010)
7. Xie, H. et al: P4P: Provider Portal for Applications. In Proceedings of ACM SIGCOMM 2008, August 17-22, Seattle, Washington, USA (2008).
8. Mengjuan Liu, et al.: An ISP-Friendly Hierarchical Overlay for P2P Live Streaming. Proceedings of 14-th IEEE International Conference on Peer-to-Peer Computing (2014).
9. Yang, P., Xu, L.: An ISP-friendly inter-overlay coordination framework for multiple coexisting P2P systems, Peer-to-Peer Network Applications, 7:396409, (2014)
10. Legout, A., et al: Clustering and Sharing Incentives in BitTorrent Systems. In Proceedings of ACM SIGMETRICS'2007, June 12-16, San Diego, USA (2007).
11. Pedro Sousa, Flexible Peer Selection Mechanisms for Future Internet Applications, Proc. of BROADNETS 2009 Conference, Madrid, Spain (2009).
12. Opsahl, T., Agneessens, F., Skvoretz, J.: Node centrality in weighted networks: Generalizing degree and shortest paths. Social Networks, vol. 32, Number 3, pp. 245-251 (2010).
13. Narayanan, S.: The betweenness centrality of biological networks. MSc Thesis, Faculty of the Virginia Polytechnic Institute and State University (2005).
14. ns2, 2011. The Network Simulator NS-2. http://www. isi.edu/nsnam/ns/.