Towards Effective Control of P2P Traffic Aggregates in Network Infrastructures

Pedro Sousa

***Abstract*—Nowadays, many P2P applications proliferate in the Internet. The attractiveness of many of these systems relies on the collaborative approach used to exchange large resources without the dependence and associated constraints of centralized approaches where a single server is responsible to handle all the requests from the clients. As consequence, some P2P systems are also interesting and cost-effective approaches to be adopted by content-providers and other Internet players. However, there are several coexistence problems between P2P applications and Internet Service Providers (ISPs) due to the unforeseeable behavior of P2P traffic aggregates in ISP infrastructures.**

In this context, this work proposes a collaborative P2P/ISP system able to underpin the development of novel Traffic Engineering (TE) mechanisms contributing for a better coexistence between P2P applications and ISPs. Using the devised system, two TE methods are described being able to estimate and control the impact of P2P traffic aggregates on the ISP network links. One of the TE methods allows that ISP administrators are able to foresee the expected impact that a given P2P swarm will have in the underlying network infrastructure. The other TE method enables the definition of ISP friendly P2P topologies, where specific network links are protected from P2P traffic. As result, the proposed system and associated mechanisms will contribute for improved ISP resource management tasks and to foster the deployment of innovative ISP-friendly systems.

***Index Terms*—Communications Software, Traffic Engineering, Network Optimization, Collaborative P2P Systems**

I. Introduction

In the last years, P2P applications [1] had been widely used in the Internet as an efficient mean to share and download resources across multiple users. This type of applications has been initially associated with the illegal share and download of copyrighted material by Internet users (e.g. music, films, etc). However, from a technical perspective, many P2P systems are underpinned by efficient resource sharing mechanisms and protocols presenting several advantages when compared with traditional centralized server approaches. In this perspective, P2P based systems also opened new opportunities in the development of enhanced Internet services allowing for more cost-effective and efficient solutions to widespread and distribute resources across a large number of end-users (e.g. as the cooperation approach presented in [6]). Many P2P systems significantly differ on their operation mode and distinct P2P applications are currently used over the Internet infrastructure. Such differences are related not only with the structured or unstructured organization nature of such systems, but also with the distinct approaches to establish peering connections and the adopted rules dictating how to transfer data among the peers participating on each particular P2P ecosystem [1]. Among several interesting solutions, the BitTorrent [2] protocol approach is a classical example of a successfully P2P use case being responsible for a relevant part of the Internet traffic [7]. Here, based on appropriately tuned incentives, peers fairly collaborate in the download of a given resource avoiding the use of costly and inefficient centralized solutions.

However, even considering that the P2P paradigm can be potentially adopted to inspire the development of advanced network and content provider applications, there is clearly a coexistence problem between P2P applications and the underlying network entities, e.g. Internet Service Providers (ISPs). There are many reasons contributing for such coexistence problems, many of which related with the unpredictable nature of the traffic aggregates generated by many P2P systems, causing that some critical links of the ISP infrastructure be traversed by considerable amounts of P2P traffic. Moreover, unnecessary inter-domain traffic can also be generated by such systems [8][20], along with the possibility that relevant congestion periods might occur at access networks. As consequence, it is common that ISPs try to limit or even block excessive P2P traffic on critical links of their infrastructures in order to avoid the cost penalties directly or indirectly induced by such traffic aggregates [14]. In addition, there are also other technical reasons that explain how harmful can some P2P traffic dynamics be for the ISP infrastructures. In fact, ISPs use many times techniques from the field of Traffic Engineering (TE) in order to optimize their infrastructures. Such techniques may help in devising appropriate capacity planning strategies, attaining near-optimal and resilient-aware routing configurations (e.g. as in [4], [5]) among many other multifaceted objectives that could be defined. Such TE mechanisms usually use as input the denominated Traffic Matrices [3], which are estimations of the overall edge-to-edge traffic that traverses the ISP infrastructure. Thus, by its unpredictable nature P2P overlay traffic makes much harder the computation of such matrices and the associated estimation errors will negatively affect the quality of all TE mechanisms that depend on traffic matrices [9] [10].

In order to mitigate the coexistence problems existing between P2P applications and underlying network infrastructures some efforts have been made within the research community, some of them advocating for the need of collaborative mechanisms and layer cooperation schemes in this specific field [15]. The proposed collaborative approaches may assume diverse perspectives, such as allowing network providers to explicitly provide valuable information to P2P applications [16] [19], the definition of inter-overlay coordination frameworks for better accommodating P2P traffic in the network [18], adding peering configuration flexibility and context-awareness to P2P

Pedro Sousa is with Centro Algoritmi and Department of Informatics, University of Minho, Braga, Portugal (email: pns@di.uminho.pt).

level entities [11] [12] or even adopting optimized hierarchical overlays schemes for P2P traffic communications [17]. Within such context, this work intends to present a contribution to this area by proposing a collaborative P2P/ISP system able to sustain the development of novel TE mechanisms fostering the coexistence between P2P applications and ISP infrastructures. The proposed system is based on a BitTorrent-like solution sustained by configurable trackers. Using the proposed system, two TE mechanisms are described being able to estimate and control the impact of P2P traffic aggregates on the ISP network links. The devised methods allow that: *i)* ISP administrators be able to foresee the impact that a given P2P swarm will have on the underlying network infrastructure and *ii)* the definition of ISP-friendly P2P distribution topologies, where specific links of the network are protected from P2P traffic. Such enhanced capabilities make possible to better control P2P traffic aggregates inside ISP network infrastructures, thus allowing to improve some ISP resource management and optimization processes. In a distinct perspective, the proposed mechanisms will also contribute to foster the development of ISP-friendly P2P systems. The proposed collaborative P2P/ISP system can be easily implemented in real network environments. Furthermore, the devised TE mechanisms are able to complement other relevant proposals and solutions made in this particular research area (e.g. [13], [16], [17], [18]).

This article is organized as follows. Section II focuses on the general architecture of the proposed collaborative system, along with the devised Traffic Engineering (TE) methods to effectively control P2P traffic aggregates in a network infrastructure. After that, Section III presents a simulation framework specially devised to test P2P/ISP collaborative mechanisms, also presenting illustrative results of the methods proposed by this work. Finally, Section IV presents the final remarks related with the developed work.

II. P2P System Architecture and Devised TE Methods

This section starts by describing the general framework underpinning the collaborative P2P/ISP system devised in this work (section II-A). Based on such framework, the following sections explore two particular Traffic Engineering (TE) mechanisms devised in this work context, namely: the estimation of the impact that the traffic generated by a given P2P swarm will have on the ISP network infrastructure (section II-B) and the possibility of attaining ISP-friendly P2P transmission topologies (section II-C).

A. General Framework

The proposed collaborative P2P system is based on some BitTorrent-like [2] principles where a group of peers (P2P swarm) cooperatively download a given resource. On this type of P2P approach when a new peer intends to join the swarm it must first contact a specific entity (entitled as P2P tracker) that will return a sample[1] of the peers actually integrating the swarm (see Figure 1). Based on such peer sample the new peer establishes contact with other peers trying to download/upload pieces of the resource in consonance with a set of choke/unchoke rules and other constrains defined within the BitTorrent protocol context [2] [21].

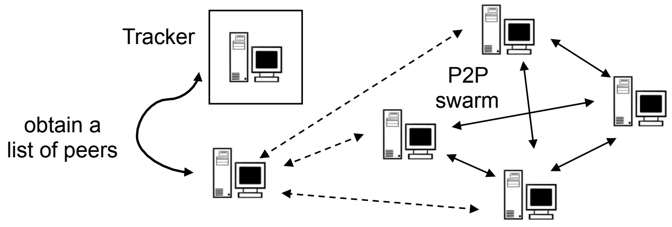

Fig. 1. A classical BitTorrent system - P2P swarm and the P2P tracker.

The framework devised in this work (depicted in Figure 2) assumes a collaborative perspective between the ISP and P2P applications. As illustrated, the network level is expected to provide valuable information to the P2P tracker that will be used in order to attain a given objective. Among a wide set of alternatives, some examples of network level inputs provided to the tracker might be: ISP topology inputs, IP routing related information along with any generic TE related data. Moreover, in the depicted framework of Figure 2 the tracker is assumed to be configurable (e.g. as in [11][12][13]) being possible that distinct peer selection mechanisms be implemented and selected during the tracker operation. Such configuration commands can be programmed by network administrators or other authorized external entities. Depending on the addressed problem the tracker may also resort to specific optimization or intelligent methods in order to attain efficient solutions. Figure 2 also highlights some components integrating the P2P tracker: a P2P traffic impact estimation module and a configurable mechanism allowing to filter the peer samples returned to the peers. Both components will be further explained in the context of the devised TE mechanisms. The framework also assumes that the P2P tracker is the only entity able to provide peering information to any peer that intends to join a given P2P swarm. Thus, client side software distributed to end-users has no capabilities to exchange peering information with other peers of the swarm.

Taking as baseline the collaborative system proposed in Figure 2, we now focus on the development of useful collaborative P2P/ISP TE mechanisms. As an illustrative case study, let's assume a scenario where a content-provider uses the collaborative P2P system to distribute a given resource among its clients. For that purpose, the interested clients should previously announce their intention to participate in the P2P swarm used distribute the mentioned resource. In this context, the P2P system supports two novel TE mechanisms that are useful from the ISP administration perspective: *i)* the ability to provide qualitative estimations of the traffic impact that a specific P2P swarm induce on ISP network links *ii)* to allow that the ISP can influence the P2P swarm dynamics in order to protect specific links of the underlying network infrastructure. As a reward for using such collaborative P2P systems, the ISP expected to give a better treatment to the traffic generated

[1] By default the tracker returns a random sample of peers to the contacting peer.

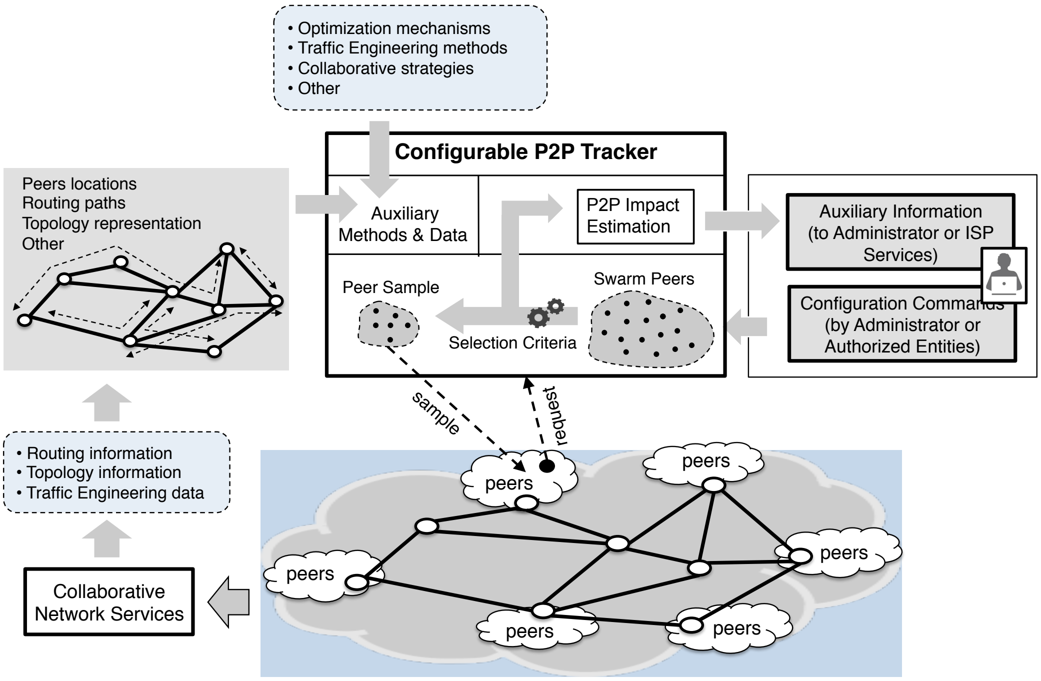

Fig. 2. General framework of the proposed system with the tracker supporting two distinct Traffic Engineering mechanisms.

by this P2P system, thus compensating this specific content-provider in opposition to other P2P approaches that will still suffer from bandwidth throttling or other restrictions usually imposed by ISPs.

B. P2P Link Impact Values

This section describes a method to attain an estimation about the impact that traffic generated by a given P2P swarm will have of the network links when involving a considerable number of peers. Thus, for a given swarm composition and taking as example the tracker behaving in the classical mode, i.e. returning a random sample of peers, the objective is to devise a method that could be used to inform the ISP administrators about the expected P2P traffic impact. Before describing the mathematical formulation sustaining the devised method a preliminary high level and very simplistic description is given based on the scenario depicted in Figure 3 a) involving several end-users areas interconnected by an ISP infrastructure. The scenario assumes a P2P swarm involving peers from three distinct areas (A,B,C) having each one a specific number of peers integrating the P2P swarm. If ones assumes the classical configuration where the tracker returns random peers samples, then it is expected that the distribution of peers among the different areas be also reflected in the returned samples. Thus, based on the peers location, corresponding distribution along the areas, and on the topology and routing information provided by ISP collaborating entities, it is possible to foresee which links from the underlying network infrastructure will be traversed by the traffic aggregates generated by the P2P swarm. In the case of the scenario depicted in Figure 3 a) let's assume the use of shortest-paths for routing decisions and the particular case where all the areas have a similar number of peers. Then, in the topology of Figure 3 a) it is expected that only network links marked with the symbols $[*]$ and $[+]$ be traversed by P2P traffic. Moreover, in this simple analysis, it is also expected that the P2P swarm will have a higher impact on the link marked with the symbol $[+]$ comparatively with the observed on the links marked with symbol $[*]$. Other complementary factors also integrating and enhancing the devised estimation model will be further described below.

Lets assume a classical mathematical representation of a network, with the graph $G = (N, L)$ expressing a network domain (e.g. an ISP network), were N is a set of the network nodes/routers and L a set of the interconnecting network links, for which routing link weights are also considered for shortest path computation. Part of the network nodes/routers might also be viewed as Points of Presence (PoP) to end-users areas having peers interested to participate in a given P2P swarm. For convenience, the location of such end-users areas is denoted by the corresponding ISP network router, a, with $a \in A$ and $A \subseteq N$. Within the scope of the proposed mechanism, several graph measures (e.g. [22], [23]) could constitute valuable inputs, in particular the concept of betweenness centrality in a graph, here adapted and extended to provide estimations of the P2P traffic impact. The devised impact estimation metric combines distinct factors that could present a preliminary snapshot of the traffic patterns exchanged within a large P2P swarm. For a specific ISP link, l, and a pair of end-users areas, $i, j \in A$, we consider the ratio between the number of shortest paths from i to j, $sp_{i,j}$, and the number of such paths that effectively pass through link l, $sp_{i,j}(l)$. By this way, each link l is assigned with a partial impact value of $\frac{sp_{i,j}(l)}{sp_{i,j}}$ for the case of peering adjacencies between areas i, j. When accounting all possible area adjacencies this metric

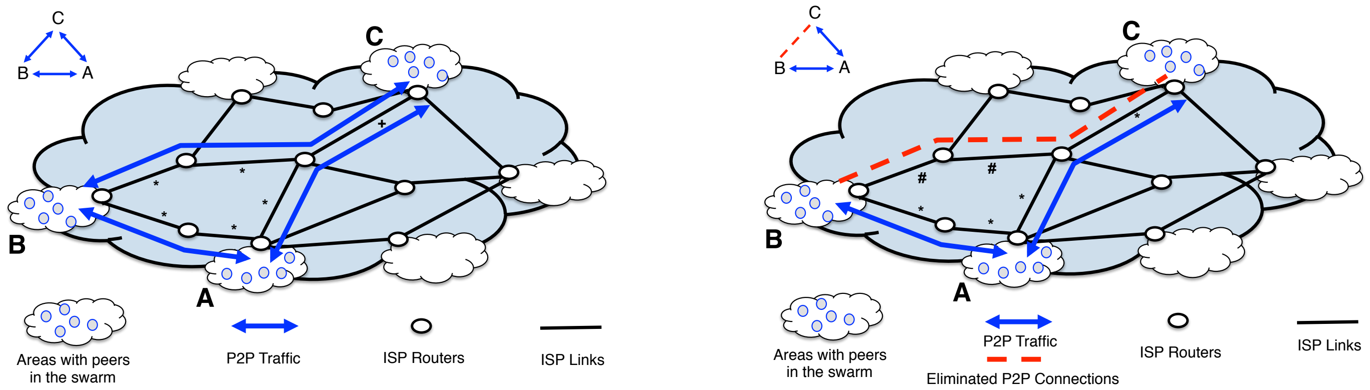
C
B
A
C
B
A
Areas with peers in the swarm
P2P Traffic
ISP Routers
ISP Links
C
B
A
C
B
A
#
#
Areas with peers in the swarm
P2P Traffic
Eliminated P2P Connections
ISP Routers
ISP Links

Fig. 3. a) Example of a network topology where several links are traversed by P2P traffic aggregates b) Example of a scenario where specific P2P connections are avoided by manipulating the peer samples returned to the peers.

will present higher values for links which integrate a higher number of shortest paths among the areas, thus having such links higher probabilities of being traversed by the P2P swarm traffic. A second weighting factor, $w_{i,j}$, is also considered for case of P2P swarms where end-user areas have an unbalanced distribution of peers. This factor considers the ratio between the number of peers involved in the peering adjacencies of areas i, j over the total number of peers involved in all possible adjacencies, favoring the importance of shortest paths connecting areas involving higher number of peers.

The above mentioned rationale can be further enhanced taking into account some characteristics of the TCP protocol that is used in the data transfers among BitTorrent peers. In fact, in such protocolar approach, peers often have a higher probability to establish peering connections with nearest peers in the network, taking advantage of lower network round-trip times (RTT). Thus, for shortest paths between areas i and j a preference value[2] ($p_{i\leftarrow j} \in [0,1]$ with $\sum_{j\in A, j\neq i} p_{i\leftarrow j} = 1$) is assigned to such adjacencies, implicitly denoting how close are areas j and i. Considering all the above mentioned reasoning, and for the case of a tracker returning random samples to contacting peers, Equation 1 presents the devised normalized P2P link impact value ($P2P_{LIV}$) value for link l, within the interval $[0,1]$. The tracker is expected to announce these estimations to ISP administrators highlighting the links that will suffer higher influence from the P2P swarm.

$$P2P_{LIV}(l) = \sum_{\substack{i,j\,\in\,A \\ i\,\neq\,j}} [(|A|-1)\cdot p_{i\leftarrow j}]\cdot \frac{sp_{i,j}(l)}{sp_{i,j}}\cdot w_{i,j} \qquad l \in L \tag{1}$$

The metric presented by Equation 1 has the major objective of gathering a preliminary snapshot of which links are expected to be traversed by higher amounts of P2P traffic. The objective is that the comparison between the $P2P_{LIV}$ values of two links can be used to foresee which one will be traversed by higher amounts of P2P traffic, i.e. that the order relations between $P2P_{LIV}$ values could also somehow express the order relation between the P2P traffic that will flow over such links. In order to validate the correctness of such impact estimations, the function $f(l,z)$ (Equation 2) is defined for two distinct links $l, z \in L$. As observed in Equation 2, the function $f(l,z)$ might return two alternative values $\{0,1\}$ according with the estimated $P2P_{LIV}$ metrics and the traffic that effectively traverses such links (function $T(l)$) after running a real/simulated experiment of the framework. If the $P2P_{LIV}$ order relations also express the $T(l)$ order relations the value returned by $f(l,z)$ is 1, otherwise 0. For the particular case of links having exactly equal $P2P_{LIV}$ values a small deviation (controlled by the γ variable) is accepted when comparing the observed traffic on each link.

$$f(l,z) = \begin{cases} 1 & \text{if } (P2P_{LIV}(l) > P2P_{LIV}(z))\&(T(l) > T(z)) \\ 1 & \text{if } \big(P2P_{LIV}(l) < P2P_{LIV}(z))\&(T(l) < T(z)) \\ 1 & \text{if } \big(P2P_{LIV}(l) = P2P_{LIV}(z))\& \\ & \qquad (T(l) \in [T(z)\cdot(1-\gamma), T(z)\cdot(1+\gamma)]\big) \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Based on the $f(l,z)$ function, Equation 3 defines now the function $\psi(l)$ expressing the order conformity of the $P2P_{LIV}$ impact value of link l. Thus, $\psi(l)$ represents the average $f(l,z)$ values obtained when directly comparing link l with all the other links of a given network topology. Therefore, $\psi(l)$ values will vary within the interval $[0,1]$, with values close to 1 expressing that most of the order relations among $P2P_{LIV}$ values also express the order relations between the P2P traffic that effectively traverses the links. This function $\psi(l)$ will be used to assess the quality of the $P2P_{LIV}$ results obtained in the experimental part of this work (Section III-A).

$$\psi(l) = \frac{\sum\limits_{z\in L\setminus\{l\}} f(l,z)}{|L|-1} \qquad l \in L \tag{3}$$

C. Attaining ISP Friendly P2P Swarms

The P2P link impact estimations previously explained are an useful asset contributing for an improved management of

[2] This value is then multiplied by the total number of distinct external areas adjacencies that could be made by peers in a given area, i.e. $|A|-1$, for normalization purposes.

network resources from the ISP point of view. In this section we proceed with an additional TE mechanism, allowing that the ISP interacts with the P2P tracker in order to influence the P2P swarm composition. Here, the main objective is to allow that the ISP protects from P2P traffic specific links of its underlying infrastructure. The underpinning concept sustaining this TE method is also summarized in a simplistic perspective in Figure 3 b). In the presented scenario it is assumed that the ISP intends to protect the links marked with the ($\#$) symbol from the P2P traffic. After receiving such information, and using the topology and routing information provided by collaborative network level entities, the P2P tracker will manipulate the peer samples provided to contacting peers in order to avoid P2P traffic from traversing such links. Thus, in the simplified example of Figure 3 b) peer samples returned to peers in area C will not include peers from area B and vice-versa.

Algorithm 1 *protecting_links_P2P_Traffic (s, K, data)*

```
1:  $X_s \leftarrow$ decreasingly ordered set with all $(a_i, a_j)$ area pairs
    having peers from swarm $s$, $a_i, a_j \in A$ {**Comment:** $X_s$ is
    a $w_{i,j} * p_{i \leftarrow j}$ ordered set}
2:  **for all** $link_l \in K$ **do**
3:      $Y \leftarrow$ decreasingly ordered subset of $X_s$ with $(a_i, a_j)$
        pairs which shortest paths include $link_l$ {**Comment:** $Y$
        is a $w_{i,j} * p_{i \leftarrow j}$ ordered set}
4:      **for all** $(a_i, a_j) \in Y$ **do**
5:          **if** $swarm\_totally\_connected(s, X_s \setminus \{(a_i, a_j)\}) =$
            $TRUE$ **then**
6:              $X_s \leftarrow X_s \setminus \{(a_i, a_j)\}$
7:          **end if**
8:      **end for**
9:  **end for**
10: $update\_tracker(s, X_s)$
```

Based on the mathematical model defined in the previous section, Algorithm 1 presents the pseudo-code of the proposed method which could be easily programmed in the tracker to attain ISP-friendly P2P topologies. As inputs this TE mechanism receives: s, a swarm identification; K, a decreasingly ordered set with all $link_l \in L$ links that the ISP wants to protect from P2P traffic (ordered by a priority assigned by the administrator in order to firstly try to divert P2P traffic from higher priority links) and $data$, auxiliary information provided by collaborative services (the network topology, the routing information, etc.). Algorithm 1 starts by considering a set with all the area pairs combinations of the network (X_s, line 1), where each pair (a_i, a_j) means that when contacted by a peer from area a_i the tracker is able to include in the random sample peers from the area a_j. If no changes are made to this X_s set the tracker will behave in the classical mode when contacted by new peers, i.e., returning a random sample of peers from all the available peers currently participating in the swarm.

Next, for each protected $link_l$, the algorithm uses the topology and routing information provided by collaborative network entities to construct the subset Y containing the (a_i, a_j) pairs for which the shortest paths connecting such areas traverse $link_l$ (line 3). The subset Y is ordered by $w_{i,j} * p_{i \leftarrow j}$ to firstly consider area pairs which are expected to generate higher volumes of P2P traffic (e.g. closer areas also having a higher number of peers). The algorithm verifies then if it is possible to remove a specific (a_i, a_j) entry from X_s in order to reduce the impact of the P2P swarm traffic on such link. The function $swarm\_totally\_connected()$ (in line 5) verifies if the swarm is still totally connected when considering that the tracker will not include peers from area a_j in peer samples sent to peers from area a_i. In this point it is important to highlight that the swarm is assumed to be totally connected if all peers have the opportunity to contact one of the swarm seeds, or contact other peers that directly or indirectly have access to the pieces sent by one of the seeds. In both cases, all the peers will have the opportunity to download all the pieces of the shared resource. Otherwise, the swarm is considered to be partitioned and some peers will never receive all the pieces of the shared file. In the case that the swarm would not become partitioned, the (a_i, a_j) pair is effectively removed from the set X_s (line 6).

As final result, Algorithm 1 computes the set X_s containing all area pairs that the tracker should consider to build random peers samples that are returned to contacting peers. As result of that, it is assured that the formed P2P swarm will have the minimum possible traffic impact on the considered protected links of the ISP infrastructure.

III. Experimental Testbed and Illustrative Results

Figure 4 describes the main modules of the simulation framework that was implemented to test the devised P2P/ISP collaborative system and the proposed TE methods. The simulation framework was implemented as an extension to the ns-2 simulator [24] and uses as baseline a patch which implements the basic peering dynamics of the BitTorrent protocol [25]. Such patch was further enriched with other modules specifically implemented in this work context. The defined modules include a tracker configuration module allowing to receive configuration commands to activate specific methods that are available in the tracker. Such configuration commands are expected to be provided by administrators or authorized external entities. In addition, in Figure 4 a collaborative network service is also available allowing to simulate the exchange of valuable information between network level entities and the collaborative P2P tracker (e.g. topology, routing and other relevant data within the context of TE mechanisms). The internal P2P tracker architecture allows to run user defined source code, allowing that any generic Traffic Engineering method could be implemented. For illustrative purposes the tracker was programmed with the TE methods previously described in Sections II-B and II-C.

A network topology is also presented in Figure 4 being used to collect illustrative results of the mentioned methods. The depicted network scenario comprises six end-users areas (from $Area_1$ to $Area_6$), interconnected by thirteen routers (from R_1 to R_{13}) which select paths with the minimum number of hops

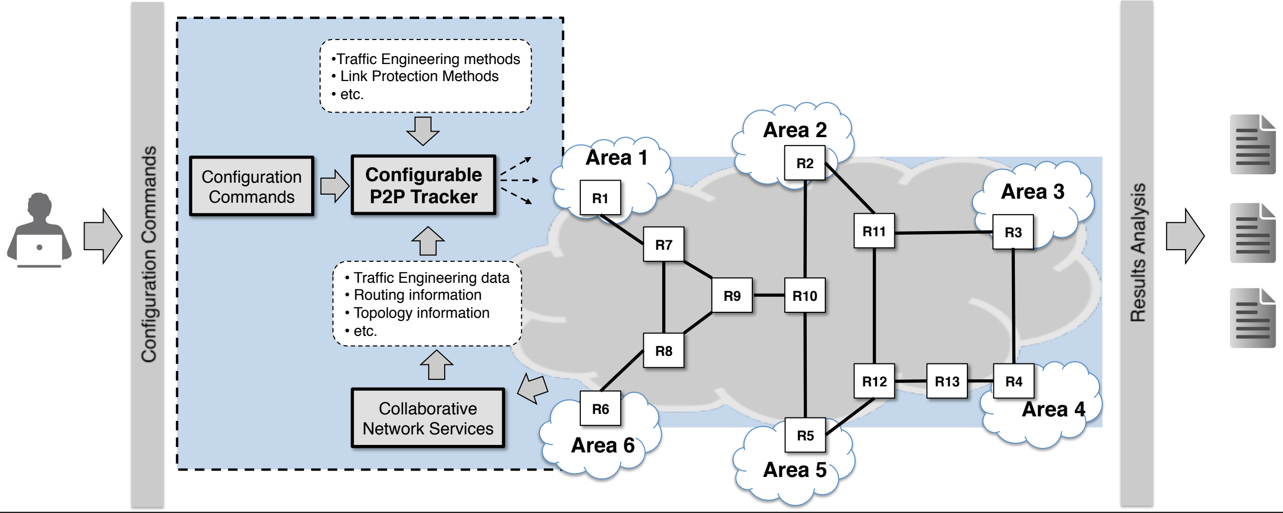

Fig. 4. Developed simulation testbed to test collaborative P2P/ISP TE mechanisms and an illustrative network topology for results analysis.

to route traffic between any source/destination network pair. The framework allows to configure several parameter of the scenario, such as the number of peers and seeds per area, the file size, the chunk size, among many others. The presented experiments assume 300 peers composing the P2P swarm which are distributed along the six end-users areas. The swarm exchanges a $50MB$ file and the used chunk size is 256 KB. The peers in each of the end-users areas have upload/download capacities of 1 and 8 $Mbps$, respectively, to simulate common residential environments with higher download capacities. The propagation delays of the peers access links vary within $[1, 50]$ ms. In this ISP/P2P collaborative scenario it is also assumed that 50 $Mbps$ of each ISP core link is reserved to carry P2P traffic of the proposed P2P collaborative system, having such links propagation delays at least two times higher than the end users access links. By default, the peer sample returned by the tracker includes 25 peer contacts. For each one of the described experiments five simulations were made and the corresponding mean values were taken for analysis.

A. P2P Link Impact Values

Based on the scenario depicted in Figure 4 several results are now presented regarding the tracker method to estimate the P2P impact on the network links. In the provided examples several scenarios were considered for distinct combinations of peers distribution in the network, P_D, and seed locations, S_L, and the obtained results are shown in Figure 5. The scenarios vary from an uniform distribution of peers in the network areas (first row of Figure 5 with all areas having 50 peers, i.e. P_D=$(50, 50, 50, 50, 50, 50)$) to other scenarios where a higher density of peers is considered to exist in specific parts of the network. The results of such additional peer distributions are presented in the other rows of Figure 5, assuming that the left, right, upper and bottom sides of the topology of Figure 4 have a higher density of peers, respectively. In addition, and for each of the mentioned P_D distributions, three distinct seed positioning scenarios are considered: *i)* all areas having one seed; *ii)* a single seed positioned in area 1 and *iii)* a single seed positioned in area 4 (first, second and third columns of Figure 5, respectively).

Each graph of Figure 5 presents the results obtained on each particular scenario. Five independent simulations runs were made for each scenario and the plotted results are averaged values, i.e. a total of seventy five simulation instances were analyzed. For comparative analysis, on each graph, the cumulative P2P traffic which traversed each link during the swarm lifetime is represented by gray filled columns (in MBytes), being the previously computed $P2P_{LIV}$ link impact estimations[3] (Equation 1) represented by a black line-plot representation (normalized values within $[0, 1]$). A detailed analysis of Figure 5 allows to verify that in all of the considered scenarios both the $P2P_{LIV}$ link values and the overall P2P traffic on each link follow a similar trend. This constitutes a preliminary indication that $P2P_{LIV}$ metric could in fact denote the relations between the P2P traffic traversing each link during the swarm lifetime.

In order to verify the correctness of the $P2P_{LIV}$ metrics, the link impact order conformity metric (function $\psi(l)$ in Equation 3) was evaluated for each one of the topology links within each one of the simulated scenarios. The obtained $\psi(l)$ values are summarized in Table I[4]. As observed the link impact metrics obtained high order conformity values. In fact, in most of the presented scenarios, and independently of the peers distribution and seed locations, the $\psi(l)$ averaged values shown in Table I fall within the interval $[0.89, 97]$. This means that, for an expressive majority of the cases, the $P2P_{LIV}$ link impact values computed by the tracker also denote the foreseeable order relations between the P2P traffic traversing each link. In that way, $P2P_{LIV}$ values can effectively be used to have a preliminary view about which links will suffer higher impact from the P2P swarm traffic, being this information a

[3] As in real scenarios the tune of $p_{i \leftarrow j}$ values is difficult, in the experiments only nearest areas are differentiated ($p_{i \leftarrow j}$=0.4), while the remaining areas have values of 0.15.

[4] For $\psi(l)$ computation (Eq. 2) variable γ was assigned with a value of 0.025, i.e. only allowing a traffic deviation of 2.5% when comparing links with equal $P2P_{LIV}$ values.

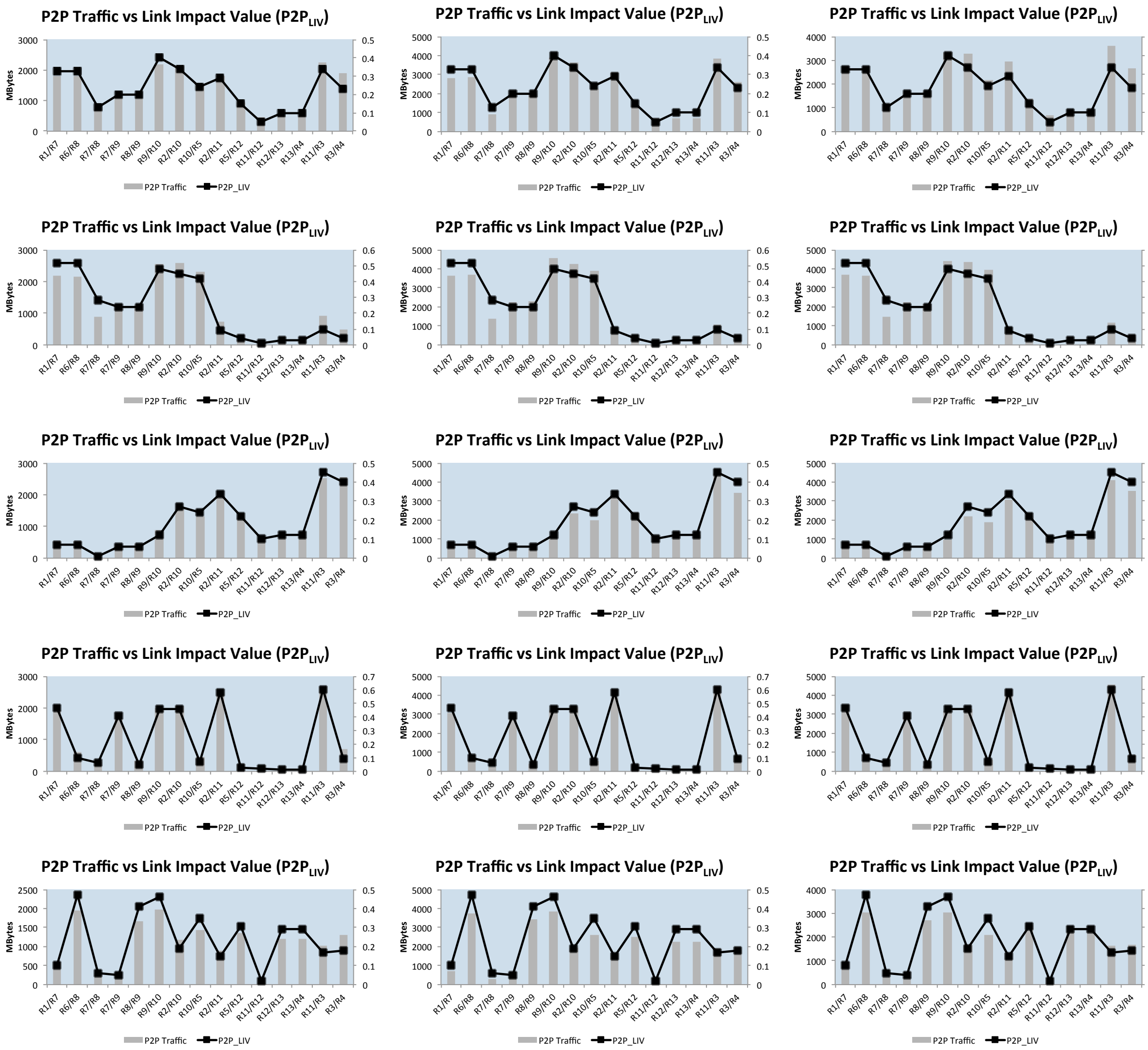

Fig. 5. P2P traffic on links vs $P2P_{LIV}$ values for distinct P_D and S_L values. Row1: P_D=(50,50,50,50,50,50); Row2: P_D=(70,70,10,10,70,70); Row3: P_D=(10,70,70,70,70,10); Row4: P_D=(90,90,90,10,10,10); Row5: P_D=(10,10,10,90,90,90); Column1: S_L=all ; Column2: S_L=A_1; Column3: S_L=A_4.

valuable asset for ISPs and network administrators.

B. *Protecting ISP Links from P2P Traffic*

The section explores the capabilities of the collaborative framework with special focus on the illustrative tracker configuration presented by Algorithm 1. Within this purpose several scenarios are analyzed (depicted in Figure 6) considering that the ISP intends to protect distinct links from the network topology. For each one of the considered scenarios, five independent simulations runs were made and the plotted results are averaged values.

1) Scenario 1: In this example the ISP notifies the tracker that specific links from the network topology should be protected from P2P traffic, in this case the blue colored links depicted in Figure 6 a) (links $R_7 \rightarrow R_9$, $R_8 \rightarrow R_9$ and $R_9 \rightarrow R_{10}$). In this scenario it is assumed to exist one seed on each networking area and all areas have the same number of peers, i.e. 50 peers. As consequence, the tracker evaluates the allowed area peering adjacencies using Algorithm 1 and the resulting rules used to build the peer samples are presented in Table II. As observed, peers from areas A_1 and A_6 are only allowed to receive in the peer samples peers also from areas A_1 and A_6, while the remaining areas are allowed to receive any peers except those from areas A_1 and A_6. With this configuration is possible to protect the selected links from the P2P swarm traffic, as required by the ISP.

TABLE II
COMPUTED PEER AREA ADJACENCIES [SCENARIO 1]

Contacting Peer	$\leftarrow$	Allowed Peers in the Sample
A_1	$\leftarrow$	$\{A_1, A_6\}$
A_2	$\leftarrow$	$\{A_2, A_3, A_4, A_5\}$
A_3	$\leftarrow$	$\{A_2, A_3, A_4, A_5\}$
A_4	$\leftarrow$	$\{A_2, A_3, A_4, A_5\}$
A_5	$\leftarrow$	$\{A_2, A_3, A_4, A_5\}$
A_6	$\leftarrow$	$\{A_1, A_6\}$

Figures 7 a) b) present the cumulative values of P2P traffic

TABLE I
LINK IMPACT VALUE ORDER CONFORMITY $\psi(l)$ ON THE SIMULATED SCENARIOS (FOR EACH SIMULATED INSTANCE OF FIGURE 5)

Scenario		**Link Impact Value Order Conformity $\psi(l)$**															
P_D	S_L	R_1 R_7	R_6 R_8	R_7 R_8	R_7 R_9	R_8 R_9	R_9 R_{10}	R_2 R_{11}	R_{10} R_5	R_2 R_{11}	R_5 R_{12}	R_{11} R_{12}	R_{12} R_{13}	R_{13} R_4	R_{11} R_3	R_3 R_4	**Avg** $\overline{\psi}(l)$
50,50,	*all*	0.86	0.86	1.00	1.00	1.00	0.93	0.93	0.93	0.79	1.00	1.00	1.00	1.00	0.86	0.71	**0.92**
50,50,	A_1	0.93	0.93	1.00	1.00	1.00	1.00	0.93	0.93	0.86	1.00	1.00	1.00	1.00	0.93	0.93	**0.96**
50,50	A_4	0.86	0.86	1.00	1.00	1.00	0.93	0.93	0.93	0.86	1.00	1.00	1.00	1.00	0.86	0.79	**0.93**
70,70,	*all*	0.79	0.79	0.79	0.93	0.93	0.79	0.79	0.86	1.00	0.93	1.00	1.00	1.00	0.93	0.93	**0.90**
10,10,	A_1	0.79	0.79	0.86	0.93	0.93	0.86	0.86	0.86	1.00	0.93	1.00	1.00	1.00	1.00	0.93	**0.91**
70,70	A_4	0.79	0.79	0.86	0.86	0.86	0.86	0.86	0.86	1.00	0.93	0.86	0.93	0.93	1.00	0.93	**0.89**
10,70,	*all*	0.93	0.93	1.00	0.93	0.93	0.86	1.00	1.00	1.00	1.00	1.00	0.93	0.93	0.93	0.93	**0.95**
70,70,	A_1	0.93	0.93	1.00	0.93	0.93	0.79	0.93	0.93	1.00	0.86	0.93	0.93	0.93	1.00	1.00	**0.93**
70,10	A_4	0.93	0.93	1.00	0.93	0.93	0.79	1.00	0.93	1.00	0.93	0.93	0.93	0.93	1.00	1.00	**0.94**
90,90,	*all*	0.86	0.93	0.93	1.00	0.93	0.86	0.86	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.93	**0.95**
90,10,	A_1	0.86	0.93	0.86	1.00	0.93	0.86	0.86	1.00	1.00	0.93	1.00	1.00	1.00	1.00	0.93	**0.94**
10,10	A_4	0.86	0.93	0.93	1.00	0.93	0.86	0.86	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.93	**0.95**
10,10,	*all*	1.00	0.93	0.93	0.93	1.00	0.93	0.93	1.00	1.00	1.00	1.00	0.93	0.93	1.00	0.79	**0.95**
10,90,	A_1	1.00	0.93	0.93	0.93	1.00	0.93	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.93	0.93	**0.97**
90,90	A_4	1.00	0.93	0.93	0.93	1.00	0.93	1.00	0.79	1.00	0.93	1.00	0.93	0.93	1.00	1.00	**0.95**

$\mathbf{P_D}$ - Peers distribution in the network (A_1,...,A_6), $\mathbf{S_L}$ - Seeds location in the network

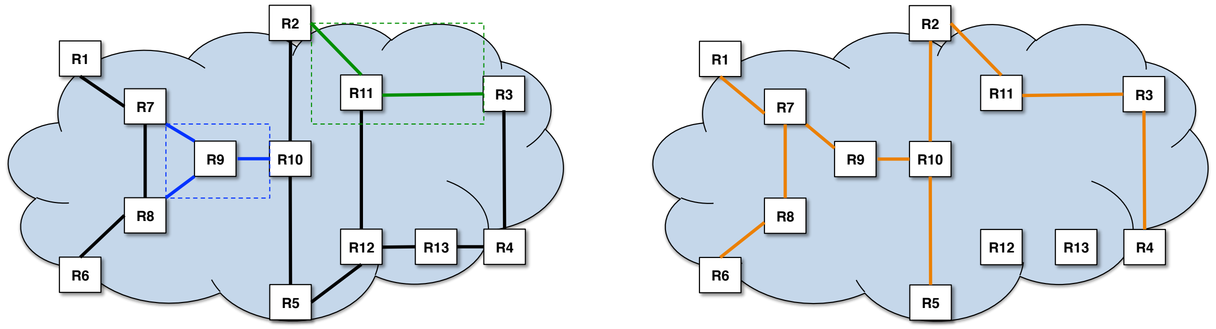

Fig. 6. a) Two network scenarios where specific links from the network infrastructure are protected (blue and green colored links) b) A virtual P2P transmission topology resulting from a tracker configuration (orange colored topology)

traversing each link of the network infrastructure. Figure 7 a) plots the results when the tracker is configured in the classical configuration mode, while Figure 7 b) shows the results when the tracker is programmed as presented by Algorithm 1. As observed, when the tracker was configured to protect the links $R_7 \rightarrow R_9$, $R_8 \rightarrow R_9$ and $R_9 \rightarrow R_{10}$ the cumulative traffic values traversing such links only show almost imperceptible values[5]. This contrasts with the observed behavior when using the default tracker configuration where the same links are traversed by a huge amount of traffic (1087, 1087 and 2175 MBytes, respectively).

2) Scenario 2: The second simulation scenario replicates the assumptions of Scenario 1, with a similar set of protected links (blue colored links of Figure 6 a)), but now considering that only one seed exists on network area 1. As consequence, and in order to maintain the P2P swarm totally connected, the tracker will devise a slightly distinct set of allowed peer adjacencies comparatively with the one previously presented

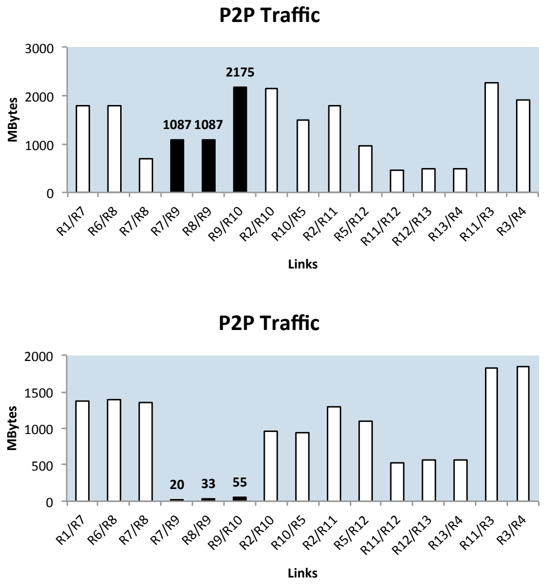

Fig. 7. [Scenario 1] P2P traffic on network links with the (a) classical tracker and (b) programmed tracker.

[5] Such residual values only appear because the tracker only uses the constraints defined by Algorithm 1 when the swarm has a sufficiently large number of peers. Before that no constraints are used when building the peers samples.

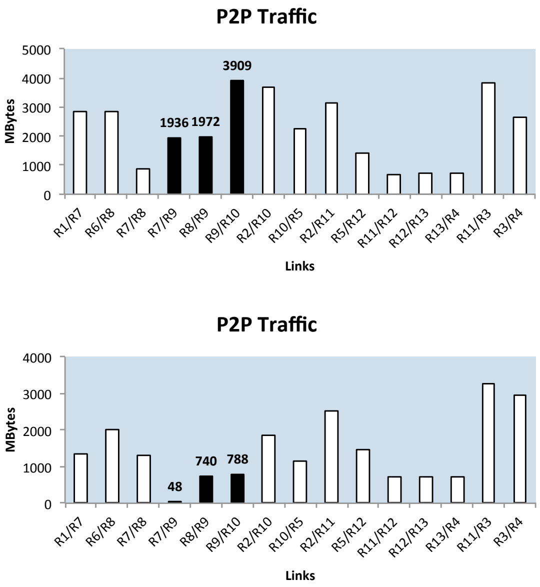

Fig. 8. [Scenario 2] P2P traffic on network links with the (a) classical tracker and (b) programmed tracker.

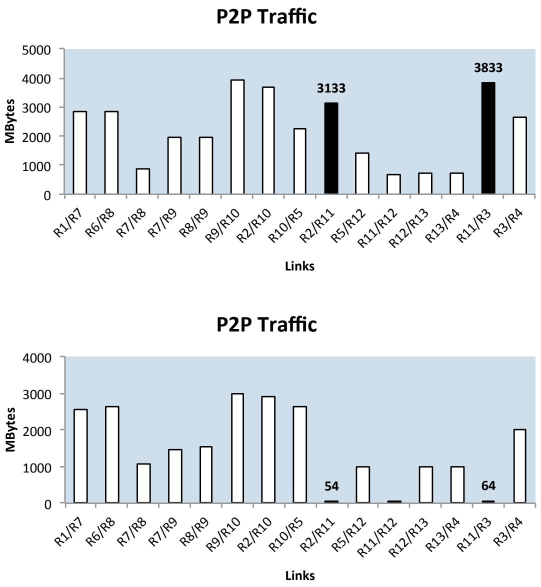

Fig. 9. [Scenario 3] P2P traffic on network links with the (a) classical tracker and (b) programmed tracker.

TABLE III
COMPUTED PEER AREA ADJACENCIES [SCENARIO 3]

Contacting Peer	$\leftarrow$	Allowed Peers in the Sample
A_1	$\leftarrow$	$\{A_1, A_2, A_5, A_6\}$
A_2	$\leftarrow$	$\{A_1, A_2, A_5, A_6\}$
A_3	$\leftarrow$	$\{A_3, A_4\}$
A_4	$\leftarrow$	$\{A_3, A_4, A_5\}$
A_5	$\leftarrow$	$\{A_1, A_2, A_4, A_5, A_6\}$
A_6	$\leftarrow$	$\{A_1, A_2, A_5, A_6\}$

TABLE IV
COMPUTED PEER AREA ADJACENCIES [SCENARIO 4]

Contacting Peer	$\leftarrow$	Allowed Peers in the Sample
A_1	$\leftarrow$	$\{A_1, A_2, A_3, A_5, A_6\}$
A_2	$\leftarrow$	$\{A_1, A_2, A_3, A_4, A_5\}$
A_3	$\leftarrow$	$\{A_1, A_2, A_3, A_4\}$
A_4	$\leftarrow$	$\{A_2, A_3, A_4\}$
A_5	$\leftarrow$	$\{A_1, A_2, A_5\}$
A_6	$\leftarrow$	$\{A_1, A_6\}$

in Table II. In this case, peers from network area 6 will be also allowed to receive in the peer sample peers from area 4, i.e. the $A_6 \leftarrow \{A_1, A_4, A_6\}$ entry should be now updated in Table II. This area pair adjacency ensures that, directly or indirectly, all peers in end-user areas have access to all the pieces of the file sent by the seed.

Figures 8 a) b) show the obtained protection levels of the links $R_7 \rightarrow R_9$, $R_8 \rightarrow R_9$ and $R_9 \rightarrow R_{10}$ in this scenario. In this example, it was not possible to fully protect all the links due to the need of assuring traffic exchanges between network areas 4 and 6. As in the previous scenario the link $R_7 \rightarrow R_9$ only shows residual values, while links $R_8 \rightarrow R_9$ and $R_9 \rightarrow R_{10}$ have cumulative traffic values of 740 and 788 MBytes, respectively (Figure 8 b)). Nevertheless, such traffic values are still significantly lower than the obtained with the classical tracker behavior presented in Figure 8 a).

3) Scenario 3: In this example the ISP instructs the tracker to protect from P2P traffic the green colored links of Figure 6 a), i.e. the links $R_2 \rightarrow R_{11}$, $R_{11} \rightarrow R_3$, for the same peers/seed distribution as in Scenario 2. After the tracker computation of Algorithm 1 the resulting rules used to build the peer samples are presented in Table III.

With the computed peer adjacencies the tracker is able to effectively divert traffic from links $R_2 \rightarrow R_{11}$, $R_{11} \rightarrow R_3$, as clearly visible in Figure 9 b). This behavior is completely distinct from the one with the tracker configured in the classical mode where the same links are traversed by a significant amount of P2P traffic (see Figure 9 a)).

4) Scenario 4: In this scenario we explore a slightly distinct optimization process made by the tracker which also indirectly uses Algorithm 1. Here, the ISP tries to define a virtual topology for P2P transmission, trying to minimize the number of links used by a given P2P swarm. For that purpose, after the request made by the ISP the tracker computed the virtual topology presented in Figure 6 b) (orange colored links). As depicted in Figure 6 b) this topology is attained by removing five specific links of the network topology which result from the peering adjacencies computed by the tracker and presented in Table IV.

As consequence, five from the fifteen ISP links (i.e. 33.3% of the infrastructure) are protected from the traffic of the P2P swarm. This behavior can be observed in Figures 10 a) and b) clearly attesting the protection of the five mentioned links when the tracker is conveniently programmed.

5) Peers Download Time: The above presented examples illustrated four distinct scenarios where the tracker was configured to protect specific links of the network topology. To achieve such objective the tracker manipulates the samples

TABLE V
PEERS DOWNLOAD TIMES VARIATIONS IN PERCENTAGE (%) [IN COMPARISON WITH THE TRACKER CONFIGURED IN THE CLASSICAL MODE]

	Area 1	**Area 2**	**Area 3**	**Area 4**	**Area 5**	**Area 6**	**Overall Swarm**
Scenario 1	+6.6%	+1.4%	0%	-0.7%	+1.2%	+5.9%	**+2.4%**
Scenario 2	-15.9%	-6.1%	-7.7%	-9.2%	-6.1%	-15.8%	**-10.1%**
Scenario 3	-8.6%	-6.9%	-4.4%	-5.4%	-6.5%	-8.6%	**-6.7%**
Scenario 4	-3.7%	-1.0%	-0.4%	-1.1%	-2.0%	-6.7%	**-2.5%**

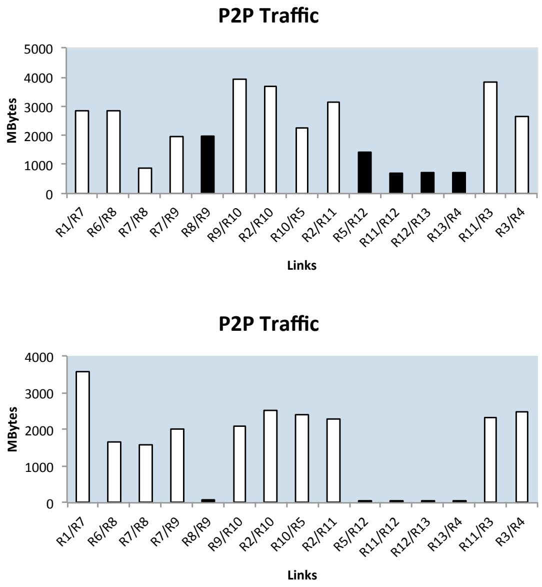

Fig. 10. [Scenario 4] P2P traffic on network links with the (a) classical tracker and (b) programmed tracker.

returned to contacting peers in agreement with the values computed by Algorithm 1. In this section, and for each of those scenarios, we analyze the time required by each peer to download the shared file and compare such values with the ones obtained when the tracker behaves in the classical mode, i.e. not imposing any restriction to the sample retuned to contacting pers. The comparison is based on five independent simulation made for each scenario, being used the averaged values for comparison.

The results presented in Table V summarize for each testing scenario the averaged peers download times variations (in percentage). The download time variations are measured on each network area and on the overall P2P swarm, i.e. an averaged value when accounting all the P2P swarm peers (last column of Table V). As expected, in the considered examples, when the tracker is configured to protect some links from the underlying network some variation exist in the peers download times, which may range from a small degradation (e.g. $+2.4\%$) to a small improvement (e.g. -10.1%) comparatively with the tracker behaving in the classical configuration. The magnitude of the observed variations clearly highlight the idea that the cost of participating in a collaborative P2P system such as the presented here could be almost negligible and sometimes it is even possible that an improvement in the download times be observed. This is explained by the fact that, depending on the considered scenario, the protection of some links induced by the mechanism based on Algorithm 1 may also have in some cases the side-effect of improving the locality of the peers connections.

IV. CONCLUSIONS

In the last years we have witnessed an increasing use of P2P based applications in the Internet. Such applications usually establish an overlay infrastructure operating over the underlying network. Moreover, P2P applications are usually based on proprietary mechanisms which rule the adopted peering decisions and the used collaborative approaches to locate and download a given resource. However, the unpredictable nature of most of the generated P2P traffic hinder the peaceful coexistence between P2P applications and ISPs.

As a contribution to this research area, this work presented a collaborative BitTorrent-like system with the ability to be used for the development of novel TE mechanisms. Using the proposed framework, two illustrative and easy to implement TE methods are proposed being able to estimate and control the impact of the traffic aggregates generated by a P2P swarm. By this way, the proposed P2P architecture and the devised TE methods allow that network administrators be firstly informed about the traffic impact that a given prescheduled P2P swarm will have on the network links of the ISP. Based on such qualitative information it is possible to foresee which links will be traversed by higher volumes of P2P traffic. Moreover, a method is also proposed allowing that network administrators be able to interact with the P2P tracker in order to attain ISP-friendly P2P distribution topologies, i.e. protecting some links of the network from P2P traffic. Both the collaborative P2P system and the devised TE methods were tested resorting to simulation and the obtained results clearly corroborate the effectiveness of the proposed system and associated mechanisms.

Acknowledgments: 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., Crowcroft, J., Pias, M., Sharma, R., Lim, S.: 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 The 2014 ACM International Conference on Measurement and Modeling of Computer Systems. 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] Pereira, V., Sousa, P., Cortez, P., Rio, M., Rocha, M.: Robust Optimization of Intradomain Routing Using Evolutionary Algorithms, 10th International Symposium on Distributed Computing and Artificial Intelligence, Salamanca, Spain, Advances in Intelligent Systems and Computing, Springer, Volume 217, pp. 201-208 (2013)

[6] Iva Bojic, Vedran Podobnik, Mario Kusek, and Gordan Jezic. 2011. Collaborative Urban Computing: Serendipitous Cooperation Between Users in an Urban Environment. Cybern. Syst. 42, 5 (June 2011), 287-307.

[7] 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).

[8] Seetharaman, S., Ammar, M.: Characterizing and mitigating inter-domain policy violations in overlay routes. In Proceedings of IEEE International Conference on Network Protocols (ICNP) (2006).

[9] Keralapura, R., Taft, N., Chuah, C., Iannaccone, G.: Can ISPs take the heat from overlay networks?. In Proceedings of HotNets-III, San Diego, CA (Nov. 2004).

[10] Qiu, L., Yang, Y. R., Zhang, Y., Shenker, S.: SelFIsh routing in Internet-like environments. In Proceedings of SIGCOMM, Karlsruhe, Germany (August 2003).

[11] Sousa, P.: Flexible Peer Selection Mechanisms for Future Internet Applications. In Proceedings of BROADNETS 2009 - Sixth International ICST Conference on Broadband Communications, Networks and Systems, Madrid, Spain (2009).

[12] Sousa, P.: Context Aware Programmable Trackers for the Next Generation Internet. In EUNICE, The Internet of the Future, 15th Open European Summer School and IFIP TC6.6 Workshop, EUNICE 2009, Barcelona, Spain, September 7-9, pp. 78–87 (2009).

[13] Sousa, P: A Framework for Highly Reconfigurable P2P Trackers, Journal of Communications Software and Systems, 9(4), 236–246 (2013).

[14] Wang, W., Wang, N., Howarth, M., Pavlou, G.: A Dynamic Peer-to-Peer Traffic Limiting Policy for ISP Networks, In Proceedings of 2010 IEEE/IFIP Network Operations and Management Symposium, pp. 317-324 (2010)

[15] Vijay K. Gurbani, Volker Hilt, Ivica Rimac, Marco Tomsu, and Enrico Marocco. A survey of research on the application-layer traffic optimization problem and the need for layer cooperation. Comm. Mag. 47, 8 (August 2009)

[16] Xie, H. et al: P4P: Provider Portal for Applications. In Proceedings of ACM SIGCOMM 2008, August 17-22, Seattle, Washington, USA (2008).

[17] Mengjuan Liu, Fei Lu, Xucheng Luo and Zhiguang Qin. An ISP-Friendly Hierarchical Overlay for P2P Live Streaming. Proceedings of 14-th IEEE International Conference on Peer-to-Peer Computing (2014).

[18] Yang, P., Xu, L.: An ISP-friendly inter-overlay coordination framework for multiple coexisting P2P systems, Peer-to-Peer Network Applications, 7:396409, (2014)

[19] Vinay Aggarwal, Anja Feldmann, and Christian Scheideler. 2007. Can ISPS and P2P users cooperate for improved performance?. SIGCOMM Comput. Commun. Rev. 37, 3, 29-40 (July 2007)

[20] Choffnes, D. R., Bustamante, F. E.: Taming the Torrent: A practical approach to reducing cross-ISP traffic in P2P systems. *In Proceedings of the International ACM SIGCOMM conference* (August 2008).

[21] Legout, A., et al: Clustering and Sharing Incentives in BitTorrent Systems. In Proceedings of ACM SIGMETRICS'2007, June 12-16, San Diego, USA (2007).

[22] 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).

[23] Narayanan, S.: The betweenness centrality of biological networks. MSc Thesis, Faculty of the Virginia Polytechnic Institute and State University (2005).

[24] ns-2 (The Network Simulator). Sources and Documentation from http://www.isi.edu/nsnam/ns/.

[25] Eger, K., Hofeld, T., Binzenhofer, A., Kunzmann, G.: Efficient Simulation of Large-Scale P2P Networks: Packet-level vs. Flow-level Simulations. In Proceedings of 2nd Workshop on the Use of P2P, GRID and Agents for the Development of Content Networks, Monterey Bay, USA (2007).

Pedro Sousa graduated in Systems and Informatics Engineering at the University of Minho, Portugal, in 1995. He obtained a MSc Degree (1997) and a PhD Degree (2005), both in Computer Science, at the same University. In 1996, he joined the Computer Communications Group of the Department of Informatics at University of Minho, where he is an Assistant Professor and performs his research activities within Centro Algoritmi at the same university. He is also member of the IEEE Professional Association and IEEE Communications Society.