IEICE TRANS. INF. & SYST., VOL.E94–D, NO.12 DECEMBER 2011

PAPER

Understanding of Network Operator-Friendly P2P Traffic Control Techniques

HyunYong LEE[†*a)], ***Nonmember and*** **Akihiro NAKAO**[††b)], ***Member***

SUMMARY In the network operator-friendly P2P traffic control technique such as P4P, peers are supposed to select their communication partners by following a guidance issued by the network operator. Thus, the guidance has significant impact on the traffic control. However, detailed performance study of available guidances is missing. Most existing approaches do not show how they affect intra-domain traffic control in detail while mostly focusing on inter-domain traffic control. In this paper, we try to understand how the guidances affect the intra and inter-domain traffic control for better guidance improving the traffic control. Through simulations, we reveal the following. The performance-based guidance reflecting the networking status shows attractive results in distributing the traffic over intra-domain links and in reducing the cross-domain traffic and the charging volume of inter-domain link compared to the distance-based guidance enforcing simple localization. However, the performance-based guidance shows one limitation that can cause unstable traffic control. To overcome the identified limitation, we propose peer-assisted measurement and traffic estimation approach. Then, we verify our approach through simulations.

key words: *P2P traffic control, network operator-friendly, performance study*

1. Introduction

The network operator-friendly P2P traffic control technique [3]–[11] has been proposed to gain control over peer-to-peer (P2P) traffic, which has recently increased significantly [1]. In this technique, peers are supposed to select their communication partners by following a guidance issued by the network operator so that the network operator can control the traffic as it wants without sacrificing P2P system performance. The existing work has shown that the network operators can successfully achieve their traffic control objectives (e.g., reduced cross-domain traffic) while the peers can actually achieve better performance with the technique than without it.

Even though the network operator-friendly traffic control techniques have different architectures, they can generate same guidances that can be grouped into two types: the distance-based guidance and the performance-based guidance [15]. The distance-based guidance reflects underlying network topology and can be generated based on topological distances (expressed in the number of autonomous systems (ASes) or router hops) and physical distance (based on knowledge of the approximate geolocation). On the other hand, the performance-based guidance reflects dynamic networking status such as minimum achievable throughput and maximum round-trip time. Different guidances may lead to different traffic control results, since the guidance affects the traffic generation of peers. However, detailed performance study of the two guidances is missing while existing work just shows its feasibility in specific environment.

The most existing work tries to turn the inter-domain traffic into the intra-domain traffic (i.e., traffic localization) while do not showing how the localized traffic impacts on intra-domain traffic control in detail. If the locality is enforced without enough consideration on intra-domain traffic, (e.g., each peer simply downloads content from the closest peer), some peers may encounter congested intra-domain links. The problem may get worse as volume of the localized traffic increases as a result of the successful traffic localization.

This paper elaborates a performance study of the guidances in intra and inter-domain traffic control for better guidance that may improve the traffic control. We conduct a series of simulations based on the network topology that is built based on our observation of real BitTorrent swarms with following techniques: BitTorrent with the distance-based guidance (DG) and BitTorrent with the performance-based guidance (PG). We also include vanilla BitTorrent (BT) as a base case where no guidance is available.

Through simulations, we reveal that the adoption of networking status in PG leads to attractive results in distributing the traffic over intra-domain links and in reducing the cross-domain traffic and the charging volume of inter-domain link compared to DG. On the other hand, DG enforcing the traffic localization without considering the networking status just shows slight performance improvement compared to BT. However, PG shows one limitation, can be called guidance dependency problem, that may cause unstable traffic control. To overcome the identified limitation, we propose a peer-assisted measurement scheme and a traffic estimation-based guidance generation approach. The simulation results show the feasibility of our guideline.

The rest of the paper is organized as follows. Section 2 explains simulation environment. Section 3 shows our main observations from the simulation and Sect. 4 discusses our guideline to overcome the identified limitation. Section 5 introduces related work and Sect. 6 concludes this paper.

Manuscript received February 22, 2011.
Manuscript revised August 8, 2011.

[†]The author is with the National Institute of Information and Communications Technology (NICT), Tokyo, 113–0001 Japan.
[††]The author is with The University of Tokyo, Tokyo, 113–8656 Japan.
[*]Corresponding author.
a) E-mail: ifjesus7@gmail.com
b) E-mail: nakao@iii.u-tokyo.ac.jp

DOI: 10.1587/transinf.E94.D.2460

2. Simulation Setup

We utilize ns-2 simulator [22] with following settings. For the network topology, we have first collected the peer addresses by joining BitTorrent swarms with more than 350 torrents downloaded from IsoHunt [23]. From this measurement, we have data of 67,697 peers. To identify AS of the peers, we use Cymru AS mapping service [24] that maps an IP address to the AS that it belongs to. In case of when the peer belongs to multiple ASes, we use the result shown first. The peers are distributed over 6,019 ASes in total. Among the ASes, we have randomly chosen 5 ASes with more than 200 peers so that we can build a topology including various inter-domain link types (Fig. 1). ASes with number in Fig. 1 are the ASes we have chosen for the simulations and remaining ASes are on routing path between the chosen ASes. We use RouteViews [26] data showing the relationship between arbitrary two ASes (e.g., customer, peer, or provider) to identify the relationship between ASes. We use FixedOrbit.com [25] service to identify the routing path between the chosen ASes. For intra-domain topology of the chosen ASes, we utilize RocketFuel [27] data. As a background traffic, we generate different amount of constant bit rate flows on intra-domain links (from 0% to 30% of link capacity) and symmetric constant bit flows between ASes (i.e., 10% of link capacity).

We use BitTorrent [2] (the number of peers returned by tracker is 50 and there are three initial seeders) and 25 MB (256 KB) sized content (chunk). Peers join a swarm randomly from 0 to 10 seconds after simulation starts and leave the swarm after completing the download. We use 1160 peers for all simulations. We set download and upload capacity of the peer as 1500 Kbps and 500 Kbps, respectively. We divide the peers into the guided peers that follow the guidance and the non-guided peers that do not follow the guidance. To study an effect of cooperation of the peers, we conduct simulations with different ratio of the guided peers (i.e., 100%, 70%, 50%, and 30%). For the sake of simplicity, DG/PG_GP indicates DG/PG with GP% of guided peers. The non-guided peers generate variable non-guided traffic in addition to the constant background traffic.

For performance comparison, we first implement BT that is used as the basis of performance comparison. For DG, we design BitTorrent tracker so that it returns neighboring peers close to a newly joining peer in terms of AS hops instead of controlling peer communications based on network distance during BitTorrent swarming. By doing this, we try to provide sufficient connectivity required for good performance in content sharing while still allowing peers to communicate with peers close to themselves [20]. For enough connectivity with outside, the tracker returns 50% of peers from inside AS and 50% of peers from outside AS. For PG, we follow the basic approach of DG while using additional information, since the basic concept of the network operator-friendly traffic control technique is to download a file from nearby peers. We use a link utilization to generate the guidance about network scope n from the perspective of network scope m during ith interval as follows.†

$$p_i^{nm} = 1 - max_{k=1,\ldots,H}\left(\frac{s_{i-1}^{l_k}}{c^{l_k} * T}\right), \quad (1)$$

where l_k is a kth link of the path from NSn to NSm, H is the number of links of the path, $s_{i-1}^{l_k}$ is total traffic volume through l_k during $(i\text{-}1)$th interval, c^{l_k} is a link capacity of l_k, and T is a time interval for guidance generation. The guided peers generate the traffic proportional to the guidance during next interval. In our simulations, T is 5 seconds.†† To control the traffic generation, we use BitTorrent's 'INTERESTED' message, since the message triggers chunk transfer if the request is unchoked.††† We implement guidance servers to maintain the allowable number of 'INTERESTED' messages that may be transmitted between an arbitrary pair of NSes.

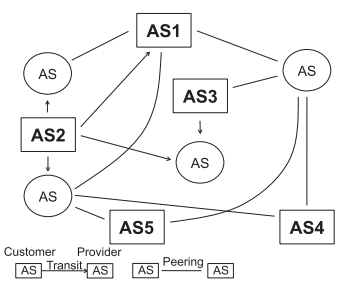


Fig. 1 Simulation topology.

3. Performance Study

We run each simulation 10 times and show the average across the results.

3.1 Intra-Domain

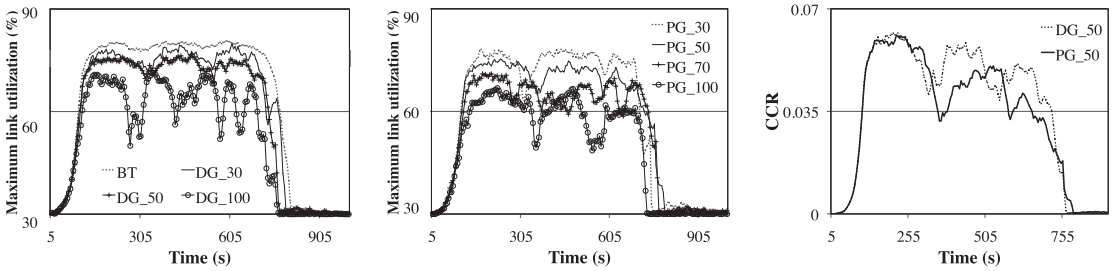
One of the main goals in the intra-domain traffic control is to distribute the traffic evenly over the intra-domain links so that the network operator can provision more bandwidth for improved services [6]. Thus, we focus on the above point. Followings are main observations that are consistent with the results from the five intra-domain topologies. In intra-domain case, NS is an IP prefix.

We first examine how much traffic is generated on intra-domain links (i.e., traffic overhead over intra-domain links). In Table 1, *IN* and *OUT* are amount of traffic that

†Network scope (NS) is a cluster sharing the same IP network prefix. For example, network scope can be IP prefix in intra-domain case and AS in inter-domain case.

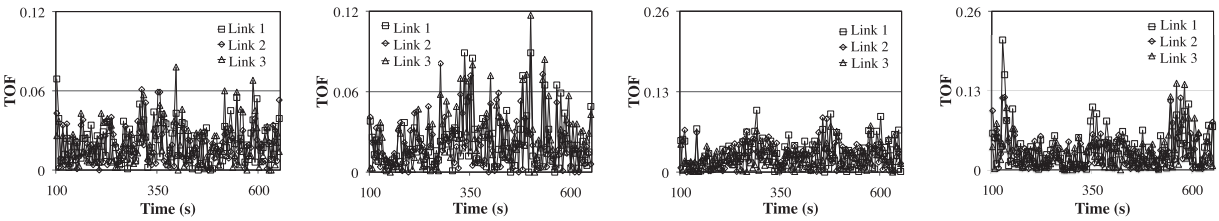
††We use 5 sec interval, since the simulation terminates around 1000 seconds. In a real world, 5 min that is a usual interval for charging volume data collection can be used.

†††We say that peer A is *unchoked* by peer B when B is willing to send data to A who issued a data request to B.



(a) MLU - BT and DG (b) MLU - PG (c) CCR

Fig. 2 Traffic distribution over intra-domain links.



(a) DG_50 (b) PG_50 (c) DG_100 (d) PG_100

Fig. 3 Guided traffic oscillation.

Table 1 Traffic overhead over intra-domain link.

	IN/OUT	Average hops
BT	0.122	1.377
DG_100	1.302	1.366
DG_70	1.036	1.382
DG_50	0.832	1.4
DG_30	0.562	1.378
PG_100	1.564	1.376
PG_70	1.08	1.376
PG_50	0.807	1.379
PG_30	0.574	1.394

is generated within same NS and from other NSes, respectively. *IN/OUT* means the ratio of IN to OUT. For example, low IN/OUT ratio means that much traffic is generated over intra-domain links. *Average hops* is the average number of intra-domain links used for downloading the chunks from the other NSes. The absence of guidance in BT results in the highest traffic overhead. On the other hand, DG and PG show less traffic overhead than BT, since the peers more often select the peers of same NS. The guidance, however, does not affect the content download path length, even though IN is much increased by the guidance. DG and PG show similar results. Basically, BT and DG/PG_100 show how the guided peers and the non-guided peers affect the traffic overhead. Even though the traffic overhead increases as the ratio of guided peers decreases, since the non-guided peers generate the non-guided traffic, DG/PG_30 show still better results than BT. Above results show that the closeness that is common in DG and PG can reduce the traffic overhead while the content download path length does not much change by the guidance.

We examine how the traffic is distributed over intra-domain links by using maximum link utilization (MLU) (Fig. 2). BT has no guidance except its peering policy. As a result, the traffic is unevenly distributed over intra-domain links, which results in the highest MLU. DG and PG show better traffic distribution compared to BT by using the guidance reducing the traffic overhead. PG shows better traffic distribution compared to DG by reflecting the dynamic networking status. Like the case of the traffic overhead, higher ratio of guided peers leads to better results. To study the traffic distribution from somewhat different aspect, we examine how the guided traffic affects the link congestion. The guided traffic is the traffic that is generated by the request of the guided peers. For this, we define *congestion contribution ratio (CCR)* as *(Guided traffic volume / Link capacity) * Link utilization*. Intuitively, an intra-domain link is more likely to be congested by the guided traffic as an link utilization is higher and a guided traffic volume is larger (i.e., high CCR value). As shown in Fig. 2 (c), PG shows lower CCR than DG, which means that PG guides the guided peers to avoid highly utilized links. Above results show that PG reflecting the dynamic networking status through the link utilization is better than DG simply preferring close peers in distributing the traffic over the intra-domain links, even though two approaches show similar traffic overhead.

To examine a stability of traffic control, we examine a degree of guided traffic oscillation over intra-domain links. For this, we define *traffic oscillation factor (TOF)* as $(\frac{D_{i-1}^{e_k}}{\sum D_{i-1}^{e_k}} - \frac{D_i^{e_k}}{\sum D_i^{e_k}})^2$, where $D_i^{e_k}$ is a traffic volume through link e_k during ith interval and e_k is a kth intra-domain link that is connected to given certain NS. Simply, high TOF value means high traffic oscillation. To show TOF, we select one NS showing representative result while most NSes show similar results. As shown in Fig. 3, PG shows higher TOF than DG, since PG generates the guidance by reflecting

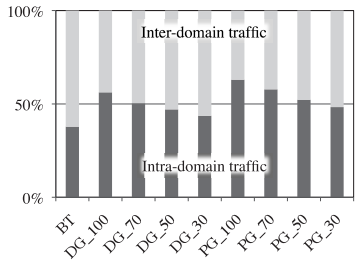


Fig. 4 Distribution of intra and inter-domain traffic.

the dynamic networking status. Intuitively, the oscillation is somewhat natural result of PG's adaptation to the dynamic networking status. We, however, observe this traffic oscillation even with static background traffic (Fig. 3 (d)). Note that there is only static background traffic in PG_100 case. The traffic oscillation problem will be discussed later in detail.

In summary, the closeness that is common in DG and PG reduces the traffic overhead compared to BT. The adoption of dynamic networking status in PG leads to the improved traffic distribution compared to DG, even though PG and DG show similar traffic overhead. PG, however, shows the traffic oscillation problem that may cause unstable traffic control.

3.2 Inter-Domain

The main goal of the inter-domain traffic control is to reduce the cross-domain traffic that can increase the operational cost. Thus, we focus on the cross-domain traffic and its relevant effect on the charging volume of transit link and the Out:In ratio of peering link. Here, NS is a AS.

We first examine the distribution of intra-domain and inter-domain traffic volume (Fig. 4). DG and PG reduce the cross-domain traffic compared to BT. In addition, PG further reduces the cross-domain traffic compared to DG. Actually, with PG, the peers try to control their traffic generation according to the guidance and thus some communications across NSes are restricted. On the other hand, the peers with DG do not have any restriction for their communications except link capacity. This result shows that the traffic localization that is common in DG and PG is the main factor for reducing the cross-domain traffic and that additional scheme of PG leads to additional improvement.

Table 2 shows how the transit traffic (i.e., traffic through the transit link) affects the charging volume. In the transit link case, the customer has to pay corresponding fee (e.g., proportional to the charging volume) to its provider providing Internet connection through the transit link. The charging volume is calculated based on the 95th-percentile charging model. DG and PG reduce the traffic through transit links and the corresponding charging volume compared to BT. In addition, PG reduces the traffic through transit links further compared to DG and this leads to the reduced charging volume.

Peering link is usually free to send traffic. There exist, however, some requirements for continuous peering relationship between NSes. Among various technical requirements of the peering link, Out:In ratio is considered as one of the most important factors to be satisfied. Thus, we examine that aspect. To examine Out:In ratio of each peering link, we choose AS4 and AS5 with only two peering links (Table 3). Even though the guidance of DG and PG does not reflect the Out:In requirement, DG and PG show improved results in most cases compared to BT. DG and PG show similar results.

Now, we examine how the traffic is distributed over two peering links in AS4 and AS5 (Table 4). Table 4 shows a ratio of traffic through one peering link to total traffic volume. Simply, high ratio indicates that much traffic is generated through one link, which means uneven traffic distribution over two peering links. PG shows improved traffic distribution compared to BT and DG as already shown in intra-domain case and supports our previous observations.

In summary, DG and PG utilizing the traffic localization in common can reduce the cross-domain traffic volume and the charging volume compared to BT. However, DG

Table 2 Traffic through transit links and charging volume.

	Transit traffic (Mbits)	Charging (Mbps)
BT	40000	251
DG_100	26227	209
DG_70	32135	226
DG_50	34576	229
DG_30	38266	234
PG_100	21668	201
PG_70	25509	208
PG_50	29104	222
PG_30	30743	226

Table 3 Out:In ratio of each peering link.

	AS4		AS5	
	Link1	Link2	Link1	Link2
BT	1.613	0.841	0.894	0.569
DG_100	0.99	1.034	0.955	1.035
DG_70	1.156	0.754	0.929	0.632
DG_50	1.213	0.658	0.902	0.579
DG_30	1.339	0.684	0.91	0.587
PG_100	1.123	1.059	0.874	0.853
PG_70	1.039	0.699	0.898	0.613
PG_50	1.037	0.598	0.978	0.586
PG_30	1.146	0.644	0.966	0.621

Table 4 Traffic distribution over peering links.

	AS4	AS5
BT	0.761	0.852
DG_100	0.677	0.677
DG_70	0.734	0.756
DG_50	0.797	0.821
DG_30	0.803	0.829
PG_100	0.568	0.599
PG_70	0.654	0.699
PG_50	0.764	0.776
PG_30	0.783	0.79

enforcing the traffic localization without reflecting the networking status just shows slight performance improvement compared to BT. On the other hand, PG improves the performance further by enabling the peers to distribute the traffic over inter-domain links.

4. Discussion

The adoption of dynamic networking status in PG leads to better traffic control than DG simply preferring close peers in intra-domain and inter-domain. PG, however, shows one potential limitation (i.e., traffic oscillation problem) as shown before. The traffic oscillation problem is caused by a guidance dependency problem where new guidance reflects networking status including the guided traffic by old guidance. In other words, the guidance (that controls generation of the guided traffic and as a result affects networking status) and the networking status (that affects the guidance generation) depend on each other. Let assume two links l_{k1} and l_{k2} with same link capacity, where $s_{i-1}^{l_{k1}} > s_{i-1}^{l_{k2}}$. Then the guidance server may give more preferable guidance to l_{k2} for ith interval. After ith interval, if $s_i^{l_{k2}} > s_i^{l_{k1}}$ by much guided traffic on l_{k2}, the guidance server may give more preferable guidance to l_{k1} for $(i+1)$th interval and this may lead to much guided traffic on l_{k1} during $(i+1)$th interval, which means an oscillation of traffic volume between two links. The guidance dependency problem may prevent the network operator from understanding networking status accurately and lead to suboptimal traffic control.

One possible approach to solve the guidance dependency problem is to distinguish the guided traffic and the non-guided traffic so that new guidance does not reflect the guided traffic by old guidance. For this, we need to measure the guided traffic and the non-guided traffic, which may cause flow-level traffic measurement and analysis overhead. Moreover, measuring the P2P traffic has various obstacles including dynamic port change and data encryption and this may result in measurement errors [17].

We propose one method utilizing the reports of guided peers to solve the guidance dependency problem while avoiding the measurement overhead and error (Fig. 5). We believe that this method can be applied to the guidance using traffic volume-related information like the link utilization. Every interval for the guidance generation, the guided peers report information about their guided traffic (including communication partner who sent traffic to themselves and corresponding traffic volume) during previous interval to the network operator. Then, the network operator can calculate the guided traffic volume of certain link, since it knows a routing path and the guided traffic is only generated by requests of the guided peers. The network operator can calculate the non-guided traffic volume by subtracting the guided traffic volume from the total traffic volume that can be acquired through SNMP query to its routers. We believe that this approach does not cause noticeable measurement overhead to the peers, since making a simple log about the received guided traffic is enough for the traffic information. This approach may allow the network operator to distinguish the guided and non-guided traffic with low measurement overhead and to generate better guidance by avoiding the guidance dependency problem.

As one application way of the peer-assisted approach for the guidance generation, the network operator may be able to estimate an allowable guided traffic volume that can be used by the guided peers for next interval (e.g., ith interval in following examples) as follows (Fig. 6):

$$g_{i-1}^{l_k} = \sum_{n=1}^{|A|} \sum_{m=1, m\neq n}^{|A|} q_{i-1}^{nm} * r_{i-1}^{l_k,nm}, \tag{2}$$

$$ng_{i-1}^{l_k} = s_{i-1}^{l_k} - g_{i-1}^{l_k}, \tag{3}$$

$$\tilde{g}_i^{l_k} = c^{l_k} * T - \tilde{ng}_i^{l_k}(intra-domain), \tag{4}$$

$$\tilde{g}_i^{l_k} = f_i^{l_k} * T - \tilde{ng}_i^{l_k}(inter-domain), \tag{5}$$

where A is a set of NSes to be considered, q_{i-1}^{nm} is the guided traffic volume from *NSn* to *NSm* during *(i-1)*th interval, $r_{i-1}^{l_k,nm}$ is 1 (if traffic from *NSn* to *NSm* passes l_k) or 0 (otherwise), $f_i^{l_k}$ is the charging volume of transit link l_k up to ith interval. The tilde means an estimated value of corresponding parameter. Firstly, the network operator distinguishes the guided and non-guided traffic by subtracting the guided traffic volume ($g_{i-1}^{l_k}$) from the total traffic volume ($s_{i-1}^{l_k}$) after calculating $g_{i-1}^{l_k}$ based on the peer reports. Then, the network operator can estimate the non-guided traffic volume for next interval ($\tilde{ng}_i^{l_k}$) by applying the existing traffic estimation technique to $ng_{i-1}^{l_k}$. For example, with the sliding window of recent N intervals [7], $\tilde{ng}_i^{l_k}$ is $\frac{1}{N}\sum_{j=i-N}^{i-1} ng_j^{l_k}$. Finally, the network operator can estimate $\tilde{g}_i^{l_k}$ by subtracting

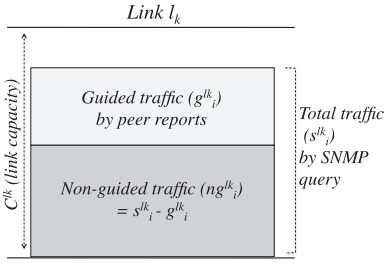


Fig. 5 Peer report-based traffic distinction.

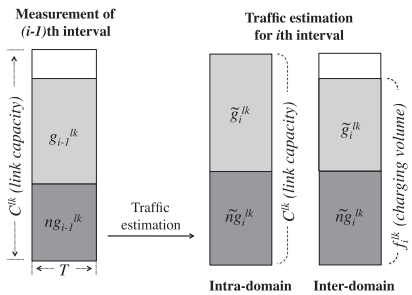
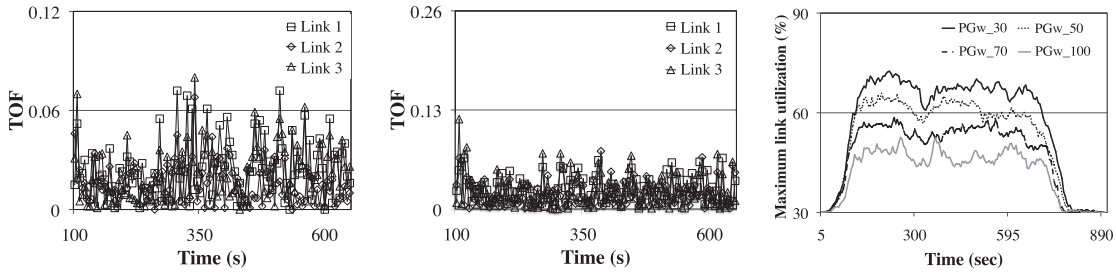


Fig. 6 Estimation of guided traffic volume.



(a) TOF - PGw_50 (b) TOF - PGw_100 (c) MLU - PGw

Fig. 7 Improvement with the guideline.

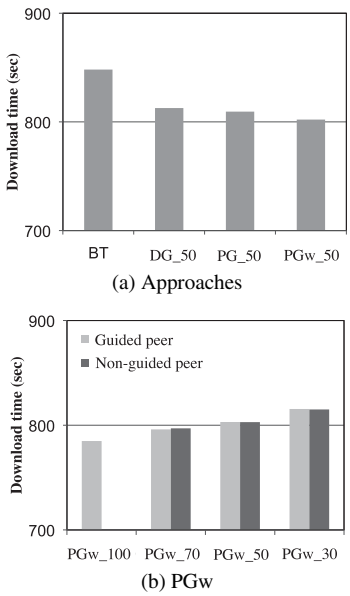
$\tilde{ng}_i^{l_k}$ from $c^{l_k} * T$ (that is an allowable traffic volume of the intra-domain link during ith interval) or from $f_i^{l_k} * T$ (that is allowable traffic volume of the transit link without increasing the charging volume). Through this way, the network operator may be able to estimate the allowable guided traffic volume as the guidance without the guidance dependency problem.

To use the peer-assisted approach, an appropriate technique needs to be applied to block false reports by malicious peers. Malicious peers can fabricate the reports while acting as the guided peers so that they can have better guidance or other peers can be interrupted. Firstly, for safe deployment, we need to limit the guided peers to authenticated peers. We also need a way to prevent the authenticated malicious peers from generating false feedback. For this, we may be able to utilize existing work that employs a cryptographic fair-exchange mechanism and shows its feasibility through an implementation [19]. With the approach of [19], each peer establishes a transport layer secure session with the guidance server (that is managed by the network operator to generate and provide the guidances) when it joins P2P network. The peer sends its ID and password over the secure channel. Then, in return, the guidance server sends a shared secret key to the peer. The shared secret key is used for peer authentication. In data exchange, the guidance server acts as the trusted third party mediating the exchange of content among peers. When a peer A uploads to a peer B, it sends encrypted content to peer B. To decrypt, B must request the decryption key from the guidance server. The requests for keys serve as the proof that A has uploaded some content to B. Thus, when the guidance server receives a key request, it credits A for uploading content to B. With this approach, the guidance server may be able to collect valid peer-level communication report with reasonable overhead.

To verify the feasibility of our guideline, we perform additional simulations with the guideline. We first examine how the guideline mitigates the traffic oscillation problem (Fig. 7).† Even though PGw still utilizes the dynamic networking information like PG, it shows lower TOF value than PG, which means that the distinction of guided and non-guided traffic leads to stable traffic control. Then, we examine how the guideline affects the traffic distribution in intra-domain. Figure 7 (c) shows that the guideline leads to better traffic distribution than PG. This result supports

Table 5 Charging volume with the guideline.

	Transit traffic (Mbits)	Charging (Mbps)
PGw_100	18639	197
PGw_70	23606	206
PGw_50	28890	217
PGw_30	33140	222



(a) Approaches

(b) PGw

Fig. 8 Download completion time.

that the guideline enables the network operator to have more accurate networking status, which leads to better guidance improving the performance. We also examine the charging volume with the guideline. As shown in Table 5, PGw reduces the amount of traffic through the transit link and the charging volume compared to PG.

In summary, PG reflecting the dynamic networking status is subject to the guidance dependency problem, which leads to suboptimal performance. On the other hand, the guideline results in additional performance improvement by solving the guidance dependency problem through the distinction of guided and non-guided traffic.

Figure 8 shows the download completion time of peers. DG, PG, PGw reduce the download completion time by

†*PGw* means PG with the guideline.

around 50 seconds (5%) compared to BT. We conjecture that a main factor for improving download completion time is the traffic localization that is common in DG and PG. This is also verified by several existing work [6], [10]. The performance improvement by DG, PG, and PGw, however, is not much in our study. We believe that the performance improvement heavily depends on the underlying network topology as well as a number of peers inside the same network domain [10]. Figure 8 (b) shows the download completion time of guided and non-guided peers under various ratios of the guided peers. Basically, the performance of both increases as the ratio of guided peers increases. One interesting observation is that the guided peers and the non-guided peers show similar performance. Even though we control INTERESTED message of the guided peers to follow the guidances, it does not degrade the performance of non-guided peers. It rather increases the performance of the non-guided peers. This result shows that controlling the message allows the guided peers to communicate with peers (including the non-guided peers) that close to themselves and have preferential guidance and thus that it leads to the performance improvement of both peers. We observe same result from DG and PG cases.

5. Related Work

There have been several bilateral cooperative approaches based on the cooperation between the network operator and the peers. In P4P [6], each peer has PID that may represent its network position like AS. The pDistance indicates the distance between a pair of PIDs (e.g., pDistance can be calculated based on BGP preferences and financial costs) and is used as the guidance. The basic idea of [8] and [9] is to provide a list of ordered peers or paths according to the predefined criteria. When a peer sends a list of possible neighbors to the network operator, the network operator ranks them according to certain criteria such as high bandwidth links. Following these approaches, the IETF has recently formed a working group for application layer traffic optimization (ALTO) [21] aiming at defining a query-response protocol between ALTO server that provides the guidance (e.g., the network operator or authorized third party) and ALTO client that queries the guidance (e.g., peers or delegated entity). ALTO client passes the list of possible neighbors to the ALTO server and the ALTO server returns the list of possible neighbors, together with the guidance. Detailed things about the guidance itself is out of scope of the ALTO working group.

Some approaches focus on verification of existing bilateral cooperative approaches under real environment and its improvement. In [3], they show the win-win approach of the network operator-friendly technique is hard to achieve under real environment where peers are non-uniformly distributed. Then, they propose refinements of current proposals, allowing all users of P2P networks to be sure that their application performance is not reduced. In [5], the authors show that transmission cost of P2P streaming with ALTO guidance can be reduced. They also show that the network operator has to be careful not to over-localize traffic, for particularly delay-sensitive applications. If peers connect to too many peers which are in the same AS but have low upload capacity, chunk loss increases considerably resulting in poor video quality.

There have also been unilateral approaches. In [4], they try to answer some fundamental questions raised by in using existing locality mechanisms (e.g., how far can we push locality?). In particular, they evaluate the impact of locality (in the peer matching of BitTorrent) on inter-domain links traffic and peers download completion time. In [10], peers use CDN's DNS redirection technique for finding their communication partners that are likely to be closer to themselves. When a peer tries to choose its communication partner, it calculates the *cosine similarity* between the ratio map (a distribution of DNS redirections) of itself and those of candidate peers and uses the results as the guidance. In [11], the authors try to minimize the inter-domain cost by calculating an AS path between arbitrary two peers and using it as the guidance to select close peers in terms of AS hops.

6. Conclusion

In this paper, we try to understand the intra and inter-domain traffic control by available guidances from the existing approaches. Through simulations, we reveal that PG shows better performance than DG in terms of various aspects in intra and inter-domain traffic control. PG, however, shows the guidance dependency problem that can lead to unstable traffic control when the dynamic networking status is used for the guidance generation. To overcome the guidance dependency problem, we propose the peer-assisted measurement scheme and the traffic estimation-based guidance generation. The simulation results verify the feasibility of guideline. We are developing the network operator-friendly P2P traffic control technique based on the guideline. In particular, we plan to study a super-peer based peer-assisted measurement to reduce traffic and computing overhead while ensuring the security.

References

[1] T. Karagiannis, D. Papagiannaki, and M. Faloustsos, "Should Internet service providers fear peer-assisted content distribution?" Proc. IMC, 2005.
[2] B. Choen, "Incentives build robustness in bittorrent," Proc. Workshop on Economics of Peer-to-Peer Systems (P2PEcon), 2003.
[3] F. Lehrieder, S. Oechsner, To. Hobfeld, D. Staehle, Z. Despotovic, and W. Kellerer, "Mitigating unfairness in locality-aware peer-to-peer networks," Int. J. Netw. Manage., vol.21, issue 1, pp.3–20, 2011.
[4] S.L. Blond, A. Legout, and W. Dabbous, "Pushing bittorrent locality to the limit," Comput. Netw., vol.55, issue 3, 2011.
[5] J. Seedorf, S. Niccolini, M. Stiemerling, E. Ferranti, and R. Winter, "Quantifying operational cost-savings through alto-guidance for p2p live streaming," Proc. International Conference on Incentive, Overlays, and Economic Traffic Control, 2010.
[6] H. Xie, Y. Yang, A. Krishnamurthy, Y. Liu, and A. Silberschatz, "P4P: Provider portal for applications," Proc. ACM SIGCOMM,

2008.
[7] H. Xie, Y. Yang, and A. Silberschatz, "Towards an isp-compliant, peer-friendly design for peer-to-peer networks," IFIP Networking, LNCS 4982, pp.375–384, 2008.
[8] V. Aggarwal, A. Feldmann, and C. Scheideler, "Can isps and p2p users cooperate for improved performance?," SIGCOMM Computer Communication Review, vol.37, no.3, pp.29–40, 2007.
[9] D. Saucez, B. Connet, and O. Bonaventure, "Implementation and preliminary evaluation of an isp-driven informed path selection," Proc. ACM CoNEXT, Dec. 2007.
[10] D. Choffnes and F. Bustamante, "Taming the torrent: A practical approach to reducing cross-isp traffic in peer-to-peer systems," Proc. ACM SIGCOMM, 2008.
[11] C.H. Hsu and M. Hefeeda, "ISP-friendly peer matching without isp collaboration," Proc. International Workshop on Real Overlays and Distributed Systems (ROADS), 2008.
[12] J.A. Pouwelse, P. Garbacki, D.H.J. Epema, and H.J. Sips, "The bittorrent p2p file sharing system: Measurements and analysis," Proc. International Workshop on Peer-to-Peer Systems (IPTPS), 2005.
[13] A. Legout, N. Liogkas, E. Kohler, and L. Zhang, "Clustering and sharing incentives in bittorrent systems," Proc. ACM SIGMETRICS, 2007.
[14] R. Bindal, P. Cao, W. Chan, J. Medval, G. Suwala, T. Bates, and A. Zhang, "Improving traffic locality in bittorrent via biased neighbor selection," Proc. IEEE ICDCS, 2006.
[15] S. Kiesel, L. Popkin, S. Previdi, R. Woundy, and Y.R. Yang, "Application-layer traffic optimization (ALTO) requirements," Internet-Draft draft-ietf-alto-reqs-00 (Work in Progress), April 2009.
[16] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks," Proc. ACM WWW, 2005.
[17] L. Jun, Z. Shunyi, L. Shidong, and X. Ye, "Active p2p traffic identification technique," Proc. IEEE Computational Intelligence and Security, 2007.
[18] M. Piatek, et al, "Pitfalls for ISP-friendly P2P design," Proc. HotNets, 2009.
[19] M. Sirivianos, J.H. Park, X. Yang, and S. Jarecki, "Dandelion: Cooperative content distribution with robust incentives," Proc. USENIX Annual Technical Conference, 2007.
[20] N. Magharei and R. Rejaie, "Overlay monitoring and repair in swarm-based peer-to-peer streaming," Proc. ACM NOSSDAV, 2009.
[21] ALTO working group charter, http://www.ietf.org/html.charters/alto-charter.html/
[22] Network Simulator ns-2, http://www.isi.edu/nsnam/ns/
[23] IsoHunt, http://isohunt.com/
[24] Team Cymru, http://www.team-cymru.org/
[25] FixedOrbit, http://www.fixedorbit.com/
[26] Route Views Project, http://www.routeviews.org/
[27] Rocketfuel, http://www.cs.washington.edu/research/networking/rocketfuel/

HyunYong Lee received the M.S. degree and the Ph.D. degree in computer science from the Gwangju Institute of Science and Technology (GIST), Korea, in 2003 and 2010, respectively. He is currently the researcher of the new generation network research center at the National Institute of Information and Communications Technology (NICT), Japan. His research interests include P2P traffic control and P2P content distribution.

Akihiro Nakao received B.S. (1991) in Physics, M.E. (1994) in Information Engineering from the University of Tokyo. He was at IBM Yamato Laboratory/at Tokyo Research Laboratory/at IBM Texas Austinfrom 1994 till 2005. He received M.S. (2001) and Ph.D. (2005) in Computer Science from Princeton University. He has been teaching as an Associate Professor in Applied Computer Science, at Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies, the University of Tokyo since 2005. (He has also been an expert visiting scholar/a project leader at NationalInstitute of Information and Communications Technology (NICT) since 2007.)