World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:4, No:11, 2010

Usage-based Traffic Control for P2P Content Delivery

Megumi Shibuya and Tomohiko Ogishi

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

***Abstract*—**Recently, content delivery services have grown rapidly over the Internet. For ASPs (Application Service Provider) providing content delivery services, P2P architecture is beneficial to reduce outgoing traffic from content servers. On the other hand, ISPs are suffering from the increase in P2P traffic. The P2P traffic is unnecessarily redundant because the same content or the same fractions of content are transferred through an inter-ISP link several times. Subscriber ISPs have to pay a transit fee to upstream ISPs based on the volume of inter-ISP traffic. In order to solve such problems, several works have been done for the purpose of P2P traffic reduction. However, these existing works cannot control the traffic volume of a certain link. In order to solve such an ISP's operational requirement, we propose a method to control traffic volume for a link within a preconfigured upper bound value. We evaluated that the proposed method works well by conducting a simulation on a 1,000-user scale. We confirm that the traffic volume could be controlled at a lower level than the upper bound for all evaluated conditions. Moreover, our method could control the traffic volume at 98.95% link usage against the target value.

***Keywords*—**P2P, traffic control, traffic localization, ALTO.

I. Introduction

RECENTLY, content delivery services including VOD (Video on Demand) and live streaming have grown rapidly over the Internet and their traffic occupies significant part of total Internet traffic. According to the analysis carried out by Cisco Systems, Inc. [1], global IP traffic will quadruple from 2009 to 2014, and the sum of all forms of video (TV, VOD, Internet, and P2P) will continue to exceed 91% of global consumer traffic by 2014. ISPs (Internet Service Providers) will be obliged to increase network equipment in order to control and forward such traffic and ASPs (Application Service Providers) providing content delivery services are obliged to increase the number of content servers and their Internet connections.

For ASPs, P2P-based content delivery architecture is recognized as a cost-effective solution since it can reduce outgoing traffic from content servers and does not need to increase the number of servers if the number of users increases. Therefore, P2P architecture is being applied to commercial content delivery services [2], [3].

On the other hand, ISPs are suffering from an increase in P2P traffic due to the following reason. A P2P node, which is called a *local peer* or a *requested peer* in this paper, downloads desired content from multiple peers including content servers, which are called *remote peers* in this paper. Such remote peers are selected in a round robin manner or at random. When most of the remote peers are located in ISPs different from that of the local peer, a lot of inter-ISP traffic is generated. Subscriber ISPs have to pay transit fees to upstream ISPs based on the volume of inter-ISP traffic.

The P2P traffic is unnecessarily redundant because the same content or the same fractions of content are transferred through an inter-ISP link several times. By applying these natures of the P2P traffic, several works have been done for the purpose of P2P traffic reduction, which are network cache [4] and P2P traffic localization [5] - [7]. Hsu et al. [5] proposed a method of using GeoIP [8], which provides the network topology to peers by sending query messages. Xie et al. [6] proposed the P4P architecture whereby the ISP and ASP cooperate with each other and the *iTracker* managed by each ISP provides the network topology to a P2P application by communicating with the *appTracker*, which corresponds to the BitTorrent tracker. The P4P architecture adopts a localization policy so that 70% of remote peers are selected within the same partition ID and 80% are selected within the same AS (Autonomous System). Although our previous work [7] is similar to [6], it definitely adopts a network side peer selection mechanism. First, a *p-Tracker*, which corresponds to *appTracker*, operated by the ASP notifies candidate peers to an ISP. Then, an *n-Tracker*, which corresponds to *iTracker* operated by the ISP, selects some peers from among the candidates considering localization. This mechanism has an advantage for the ISP because it can control traffic without disclosing the network information which may include the ISP's policy and business relationship between other ISPs.

The existing works described above achieve localization by controlling the ratio of remote peers within the same network segment. We call this method *ratio-based traffic control*. This method has the characteristic that the traffic of all links including the inter-ISP links increases proportionally to the number of users that uses a P2P content delivery service. Hence, the method cannot control the traffic volume of a certain link. For example, it cannot control traffic volume for a month within 1TB or average bandwidth for every 5 minutes within 10Mbit/s.

Megumi Shibuya is with KDDI R&D Laboratories Inc., Saitama 356-8502 JAPAN. She is now with the Graduate School of Information Network Systems, the University of Electro-Communications, Tokyo 182-8585 JAPAN (phone: +81-49-278-7554; fax:+81-49-278-7839; e-mail: shibuya@ kddilabs.jp).

Tomohiko Ogishi is with KDDI R&D Laboratories Inc., Saitama 356-8502 JAPAN. (e-mail:ogishi@kddilabs.jp).

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

Upstream ISPs provide transit in various pricing policies such as fixed pricing, usage-based pricing and average usage-based pricing. In the case of usage-based pricing, typically a fee table that specifies the fee corresponding to the total traffic volume in one month is used. An example of the fee table is shown in Table I. Since the subscriber ISP is charged an excessive amount if the used traffic volume exceeds a threshold value, the subscriber ISP wishes to control traffic volume for a link so that it does not exceed the preconfigured upper bound value, which we call the *target value*.

TABLE I
EXAMPLE OF USAGE-BASED PRICING POLICY

Traffic volume[TByte]	price[dollar]
100 -	200,000
50 - 100	100,000
15 - 50	50,000
6 - 15	10,000
0 - 6	5,000

In order to solve such an ISP's operational requirement, we propose a method to control traffic volume for a link within the target value. The method is called *usage-based traffic control*. As the P2P applications under control, we assume the applications using the BitTorrent protocol; however, our methods can be applied to various P2P applications including applications with pure P2P architectures. In BitTorrent, a peer that wishes to download a content file searches remote peers via a tracker and gathers fractions of a content file from the multiple remote peers. Our method assumes that a P2P application requests *n-Tracker* to select remote peers as well as [7]. The *n-Tracker* should be improved to have usage-based control functions. The traffic volume can be controlled by deciding the number of remote peers that use the link. Concretely speaking, for each request, the *n-Tracker* should calculate the number of remote peers so that the cumulative traffic volume at the time t_i is under the target value $T_H(t_i)$. The cumulative traffic volume is managed by the improved *n-Tracker*.

The contributions of this paper are two folds. First, we propose a usage-based traffic control method that may solve the ISP's operational requirement to control traffic for a usage-based charged inter-ISP link. We also propose additional functions necessary for the improvement of existing works. Second, we evaluate that the proposed method works well using a simulation on a 1,000-user scale. We confirm that the traffic volume can be controlled at a level lower than the upper bound for all evaluated conditions. Moreover, our method could control the traffic volume at 98.95% link usage against the target value by inferring cumulative traffic volume.

This paper is organized as follows. In Section 2, we explain the BitTorrent protocol and ratio-based traffic control as a method of existing works. In Section 3, we present the design of our proposal for usage-based traffic control. In section 4, we describe the experimental evaluation of usage-based control based on a simulation study on a 1,000-user scale. In section 5, we discuss operational issues and applications of our method. Finally, we conclude the work in Section 6.

II. BitTorrent and ratio-based traffic control

A. BitTorrent Protocol

We describe the detail of the BitTorrent protocol [9] which has been prevailed over the world wide as the base protocol of various applications for P2P content delivery. Our proposal and experiment described in later sections assume that BitTorrent is used for P2P content delivery.

BitTorrent has a hybrid P2P architecture, which consists of a central control server called *tracker* and peers. The content server that provides original content is another component which can reside in the tracker.

We look over the behaviour of the BitTorrent protocol. When a peer wishes to download new content, it obtains a torrent file that contains the metadata of a content file and the tracker's address from a Web page and then requests the peer list to the tracker. The tracker responds to the peer with the list of peers selected from the peer table. The peer table is managed by the tracker and updated when a new peer requests a content file.

The peers in the list are selected from the peer table in a *network-unware* manner such as round robin or at random. The requested peer receiving the peer list tries to establish a TCP connection with the remote peers in the peer list. Each remote peer accepts the connection request when the number of established connections is lower than a predefined value.

A content file is divided into pieces and each piece is further divided into sub pieces. The piece is a unit that a peer notifies the possession of it to remote peers with the piece map and the sub piece is a unit that can be independently transferred between peers. The size of a piece and sub piece is normally 256KB and 16KB, respectively. Each pair of peers exchanges the piece map indicating which piece the peer already has using a *Bitfield* message. However, when the peer has all the pieces or none of them, it sends *Have_all* or *Have_none* message, respectively. When a new piece is added to the piece map, the peer updates a *Bitfield* and notifies with a *Have* message. The peer receiving this message notifies willingness to download by *Interested/Not_interested* messages.

Next, when the peer receives an *Interested* message, it notifies non-acceptance/acceptance of uploading by *Choke/Unchoke* messages. The *Choke* and *Unchoke* messages are sent based on *tit-for-tat* and *optimistic unchoke* strategies. In *tit-for-tat*, the remote peers from which the requested peer can download at a higher rate are selected in higher priority. The download rates of remote peers are measured at the requested peer. In *optimistic unchoke*, remote peers that are not selected by *tit-for-tat* are randomly selected. The number of remote peers selected by these strategies is predefined: typically 3 for *tit-for-tat* and 1 for *optimistic unchoke*. The selection is performed at a fixed time interval, for example, every 10 seconds.

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

B. Ratio-based Traffic Control

As described above, existing BitTorrent protocol selects remote peers in *network-unaware* manner. Therefore, it may cause unnecessarily redundant inter-ISP traffic. In order to reduce such traffic, several *network-aware* peer selection methods, by which remote peers are selected using network information provided by an ISP, are proposed. In this section, we describe ratio-based traffic control commonly applied to the existing *network-aware* methods and give a detailed explanation using our previous work [7] as an example.

A ratio-based traffic control method selects remote peers using network information such as network prefix, AS number, link cost and so on. Generally, remote peers that are located near the requested peer are selected in higher priority.

The *n-Tracker,* which is a network information management server, has a function of collecting the network information from routers or other network equipment. The *n-Tracker* is operated by an ISP and it is deployed to each segment, which specifies a network partition such as subnet ID, OSPF area or AS number, as shown in Fig. 1. The *p-Tracker* corresponds to the BitTorrent tracker. It differs from the BitTorrent tracker in that it does not directly respond to the peer request but forwards the request to the *n-Tracker*.

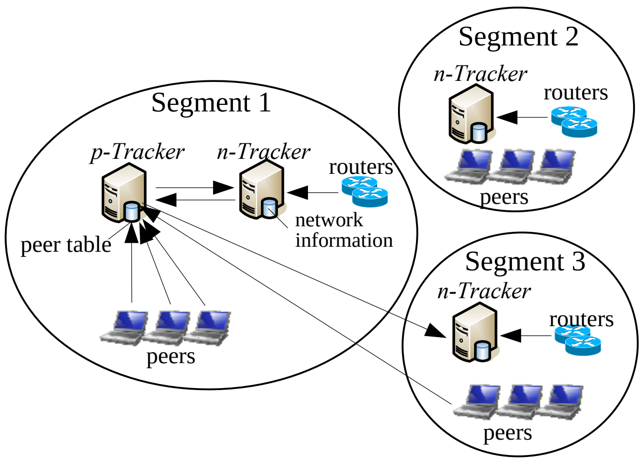

Fig. 1 Architecture of network-aware P2P content delivery system

The peer list created by the *n-Tracker* is illustrated in Fig. 2. The *n-Tracker* selects $m*S_r$ peers at first from among peers within the segment, where m is the number of *remote peers* to be selected and S_r is the *local selection ratio* which means the ratio of peers within the same segment. The S_r value is determined by the ISP based on its policy and operation know-how. By using a larger value for S_r, the ISP can reduce inter-ISP traffic although there is drawback that the propagation of content files becomes slower. Other $m*(1-S_r)$ peers are selected from peers outside the segment at random. If there are not enough peers within the segment, the peers outside the segment are selected additionally. When the number of remote peers is less than m, all candidate peers are included in the peer list. The peer list which each peer is explicitly prioritized is sent from the *n-Tracker* to the *p-Tracker*, and then forwarded to the requested peer.

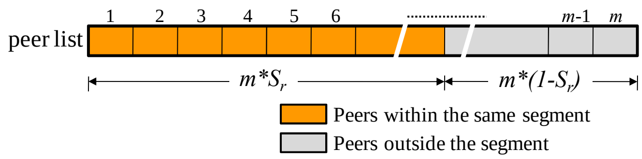

Fig. 2 Selection of peer list in ratio-based traffic control

III. Proposal of Usage-based Control

We propose a usage-based traffic control method for network-aware P2P content delivery considering the following requirement from ISP's perspective.

When an ISP purchases transit from an upstream ISP, the upstream ISP may apply a usage-based pricing policy. As a typical example of a pricing policy, a fixed price is used for a range of traffic volumes as shown in Table I.

Here, we assume that the transit fee is the same where the downlink traffic volume for a month is in the range from T_L to T_H. At this time, a subscriber ISP is willing to consume up to T_H as far as possible in order to use the transit more efficiently. Existing ratio-based traffic control methods cannot be used for this purpose because the traffic volume for a target link increases in proportion to the number of users downloading or viewing content. In order to realize traffic control of a target link, we propose a usage-based traffic control method, which controls the cumulative traffic volume for a constant duration so that it is within the target range of values.

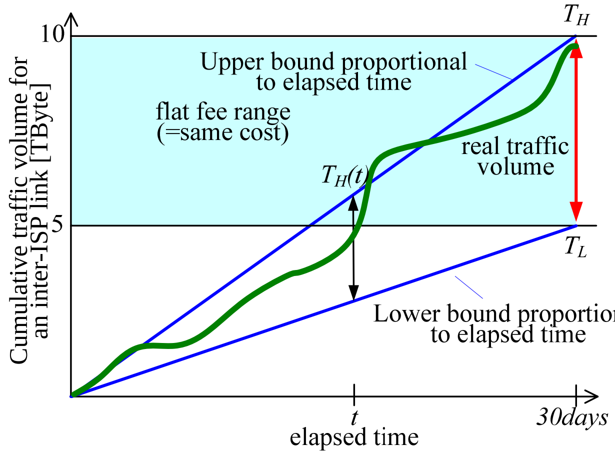

Fig. 3 Concept of usage-based traffic control

Fig. 3 shows a concept of usage-based control considering the case where the traffic volume of the target link for a month is controlled within the range from T_L to T_H. In order to realize this, the subscriber ISP has to manage the cumulative traffic volume of the link and consume the traffic volume in proportion to the elapsed time.

In this paper, we focus on the upper bound target only because upper bound target is more important than the lower bound target for the subscriber ISP's cost.

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

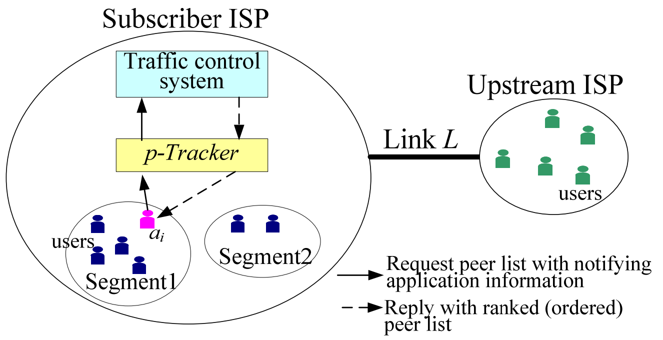

Fig. 4 Architecture of usage-based traffic control system

Fig. 4 shows the architecture of a usage-based traffic control system. The subscriber ISP deploys a traffic control system in its network. It manages the traffic volume for the inter-ISP link *L* between the ISP and an upstream ISP from which the subscriber ISP purchases transit. The *p-Tracker* provided by an ASP can be anywhere in the Internet. In this figure, it resides in the subscriber ISP. The users are downloading the same content using a P2P content delivery system. The traffic volume of link *L* can be controlled by introducing usage-based peer selection when users within segment1 and 2 request a peer list.

This traffic control system should have the following functions in order to realize usage-based traffic control.

1) Policy management:
   Configuration and management of the operation policy such as the traffic volume of each link described in the policy table
2) Network information management:
   Collection and management of the network information from routers using BGP or OSPF messages
3) Cumulative traffic management:
   Management of the cumulative traffic volume and upper bound target
4) Peer list selection:
   Peer selection policy for limiting the number of peers within a specific network segment such as an upstream ISP
5) Receipt of application information:
   Receipt of application information such as content size using the interface between ISP's and ASP's systems

Link	Direction	Period of time	Target volume [TByte]
AS1-AS2	Down	1 month	5<=T<10
AS1-AS3	Down	3 month	10<=T<15
AS1-AS3	Down	1 month	T<5
:	:	:	:

Fig. 5 Example of policy table

Fig. 5 shows an example of a policy table used in the policy management function. Several policies for each link can be applied at the same time.

The details of the traffic control method are described as follows. Fig. 6 shows the flow of the traffic control procedure, and Fig. 7 shows the method for managing the cumulative traffic volume.

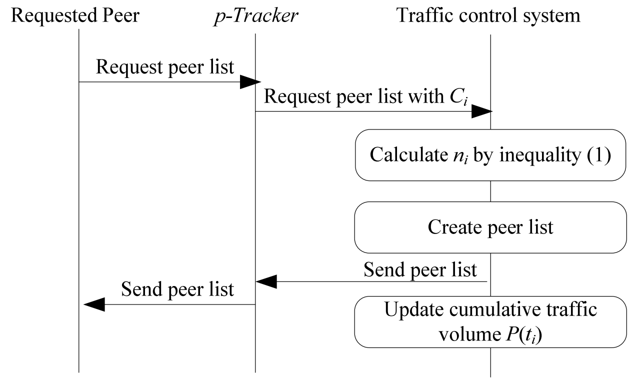

Fig. 6 Flow of traffic control procedure

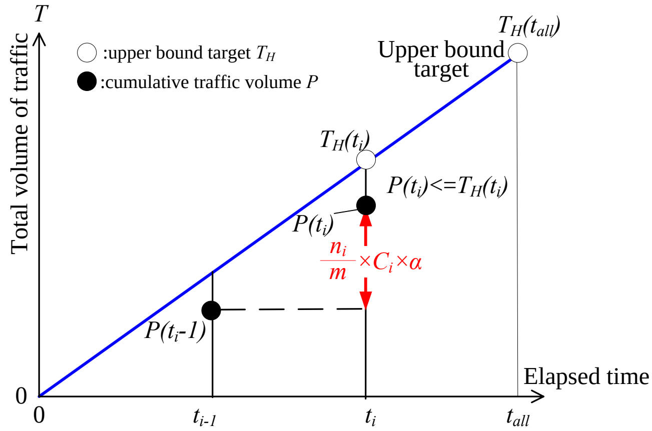

Fig. 7 Management of expected cumulative traffic volume

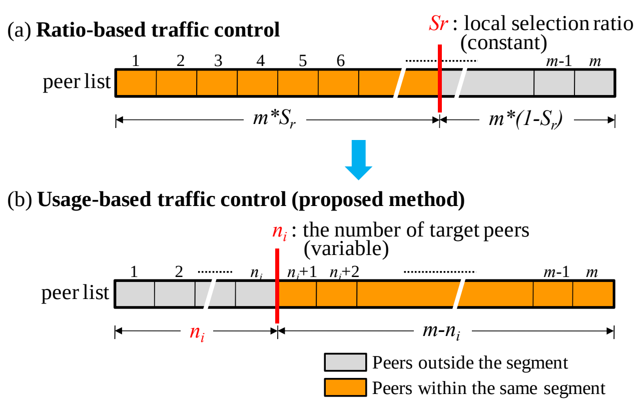

Fig. 8 Usage-based peer selection

Upon each request for the peer list from *p-Tracker*, the traffic control system searches for target peers that may consume the target link when the requested peer downloads pieces of content by using the network information the system maintains, and calculates the number of target peers to be selected so that the traffic volume does not exceed the upper bound $T_H(t_i)$ at the elapsed time t_i.

The system calculates and manages the inferred cumulative traffic volume as if the traffic volume is consumed in

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

proportion to the ratio of selected target peers among the total selected peers. First, we assume that each peer request occurs at time $t=\{t_1, t_2, \ldots, t_n\}$, where the i-th request occurs at time t_i. When the cumulative traffic volume of link L at time t_{i-1} is $P(t_{i-1})$, the traffic control system calculates the largest value of the number of target peers n_i that meets the inequality (1);

$$P(t_i) = \left(P(t_{i-1}) + \frac{n_i}{m} \times C_i \times \alpha \right) < T_H(t_i). \quad (1)$$

, where m is the number of selected remote peers, C_i is the size of i-th content file notified by *p-Tracker*, α is the parameter for compensation (discussed in later sections). The inequality is evaluated each time the traffic control system receives the request and the new inferred cumulative traffic volume $P(t_i)$ is calculated.

As shown in Fig. 8, in ratio-based traffic control, *n-Tracker* selects prioritized peers within the same segment at first, then, it selects other peers outside the segment at random. On the other hand, in usage-based traffic control, the traffic control system selects n_i target peers at random at first. Then, it selects m-n_i peers within the same segment as the requested peer in higher priority considering the localization. The peer list is sent from the traffic control system to peer a_i through *p-Tracker*. Since it selects the prioritized peers and sets them in the peer list, not only is traffic controlled at link L, but it is also localized within the subscriber ISP. As shown in Fig. 7, this process is repeated and evaluated at a constant interval (e.g. one month), according to the ISP's contract on payment. In this figure, t_{all} corresponds to the payment interval.

We developed the traffic control system including the functions 1)-5) described above based on the *n-Tracker* we had already implemented.

IV. Experimental Evaluations

In order to validate the effectiveness of our proposed method, we evaluated the traffic volume using a P2P simulator [10], which simulates the P2P content delivery based on the BitTorrent protocol for the 10,000-peer scale.

A. Network Model

The network model we have evaluated is shown in Fig. 9. In this figure, AS1 and AS2 correspond to subscriber AS and upstream AS, respectively. The traffic control system (*n-Tracker*) is operated by AS1 and *N1* and *N2* users using the P2P content delivery service are in AS1 and AS2, respectively. The propagation delay between AS1 and AS2 is set to 10 msec. In the real environment, AS1 may connect to multiple ASes (i.e. AS2, AS3, …) and have to control traffic for each link between each AS. To simplify the issue, in this paper, we had several limitations to the evaluations. First, we evaluate the case where only one upstream AS exists. Second, we evaluate only download traffic (i.e. the traffic from AS2 to AS1). We expect the result will not be so different if our evaluations are applied to multiple ASes or both directions.

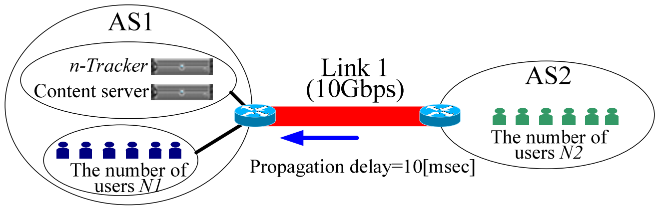

Fig. 9 Network model

Usage-based traffic control was applied to only users of AS1. In other words, the traffic control system provided the selection of remote peers when users of AS1 requested the content file and the BitTorrent tracker selected remote peers at random without considering the network information when users of AS2 requested the content file.

As the number of users in AS1 and AS2, we evaluated two conditions where the users' distributions were *N1:N2*=4:1 and 1:4. We used a single content in the simulation and assume that the ratio of users in both ASes was maintained to be constant during the evaluation time. In order to realize this, the peers in AS1 and AS2 requested the content file every 1 and 4 seconds, respectively, where *N1:N2*=4:1. We configured the system such that the peers existed in the P2P network as seeders to contribute uploading to other leechers for 800 seconds after downloading is finished. By using this mechanism, we could create an environment in which 1,000 peers constantly participated in the P2P network. We started evaluation including the measurement of cumulative traffic volume after 1,000 peers became active.

We set evaluation period as 30 minutes. Since our method is not influenced by the time scale, the result will be the same if it is applied to one month evaluation. Other parameters are listed in Table II.

TABLE II
Experimental Parameters

Parameter	Value
The number of peer list (m)	10
Size of content file (C)	100MByte
Evaluation time (t_{all})	1,800 sec (=30 minutes)
Target value at elapsed time t_{all} ($T_H(t_{all})$)	4GByte
Total number of peers (N)	2,250 (*N1*:*N2*=1,800:450=4:1, *N1*:*N2*=450:1,800=1:4)
Peer request interval Peer termination	1 sec for *N1* and 4 sec for *N2*, and vice versa 800 sec after downloading finished
Number of peers selected by *tit-for-tat*	3
Number of peers selected by *optimistic unchoke*	1

B. Experimental Evaluation

1) Effectiveness of usage-based traffic control

To validate the effectiveness of usage-based traffic control, we compared the case where usage-based traffic control is applied to that when it is not applied. In the evaluation, we used $\alpha = 1$ for inequality (1).

The results were shown in Fig. 10 and Fig. 11 in different vertical axis scales. In Fig. 10, the real traffic volumes where

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf

traffic control is not performed are specified. The straight line shows the upper bound target at time t_i, which is specified by $T_H(t_i)$. As is clearly shown in Fig. 10, the traffic volumes of uncontrolled cases exceeded the upper bound target. On the other hand, the traffic volumes where usage-based control was applied became lower than the upper bound target. From these results, we confirmed that our proposed method effectively controls traffic.

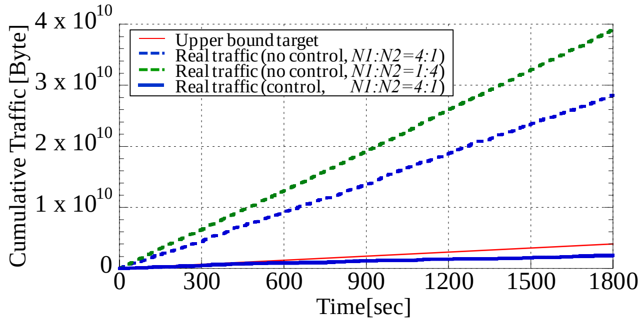

Fig. 10 Comparison between usage-based control and non-control

However, we recognized a problem wherein the traffic was reduced excessively when we applied usage-based control using $\alpha = 1$. The traffic volume was 53.35% against the target value in the case of *N1:N2*=4:1.

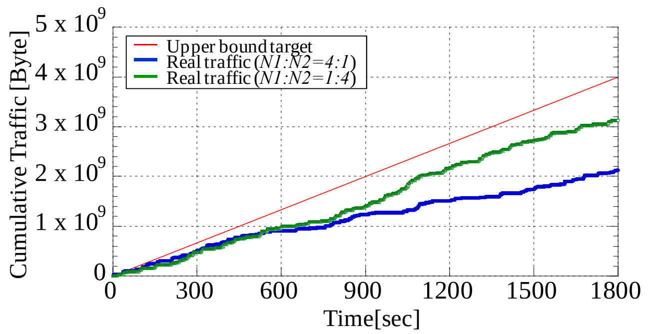

Fig. 11 Traffic volume changes where usage-based control is applied

We analyze the reason why the traffic was extremely reduced as follows. In the evaluation, we only controlled the number of selected target peers. In the BitTorrent protocol, whether the sub pieces are transferred or not is decided by the *choke/unchoke* state of each peer as described in Section 2. The peers which experience a lower download speed are inclined to be *choked*. In the evaluation, the peers of AS2 were *choked* in higher probability due to the propagation delay. Most of the peers in AS2 were not selected by *tit-for-tat* but by *optimistic unchoke*. The probabilities that peers of AS2 were selected were 200/1,000=1/5 where *N1:N2*=4:1 and 800/1,000=4/5 where *N1*:*N2*=1:4, respectively.

From the consideration above, the real traffic volume was influenced by the ratio of the peers in both ASes. The more the peers exist in the upstream AS, the closer the cumulative traffic volume becomes to the upper bound target.

2) Evaluation using the parameter for compensation

In the evaluation above, we validated usage-based control using $\alpha = 1$. As a result, we confirmed the traffic control was influenced by the number of peers in both ASes due to the behavior of *tit-for-tat* and *optimistic unchoke*. We inferred that if the traffic control system could obtain the distributions of peers between both ASes, we could control traffic closer to the upper bound target. We evaluated the traffic control by varying α. We set $\alpha = 4/5, 1/5$ in case *N1*:*N2*=4:1, 1:4 respectively considering that the probability that the peers in AS2 are not selected is $\alpha = 1 - (n/m)$.

Fig. 12 shows the real traffic when α is set appropriately. As a result, the cumulative traffic volume T_H became under the upper bound target, which were 95.20% and 98.95% against the upper bound target, respectively. We could obtain better results which ISP could use almost all the traffic volume of a specific link at almost the configured target value by selecting a suitable value for the parameter for compensation.

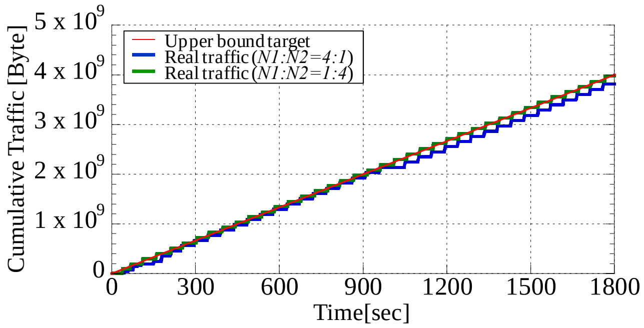

Fig. 12 Cumulative traffic volume using α

V. DISCUSSION

This usage-based traffic control method needs some information such as content size from P2P applications in order to control traffic. The framework and the information exchange model that allow the application and network to cooperate with each other are being debated in IETF ALTO (Application Layer Traffic Optimization) WG [11]. We expect that our proposed method becomes feasible according to the growth of the framework and the standardization activity.

Meanwhile, information such as the content size may not be provided by the P2P application. In this case, the traffic may be reduced extremely against the ISP's intention. In order to resolve this situation, we assume that our method can control traffic by monitoring realtime traffic information from routers.

Futhermore, our proposal in this paper was applied to P2P content delivery to download one content file from multiple peers. In principle, our method can be applied to a traditional CDN (Content Delivery Network) that does not use P2P-based delivery. In CDN, the same usage-based traffic control method can be applied and the model is rather simple because only one remote peer exists and there is no need to consider *tit-for-tat* and *optimistic unchoke*.

VI. Conclusions

In this paper, we described a usage-based traffic control method that may solve the ISP's operational requirement to control the traffic of a usage-based charged inter-ISP link. This method controls the cumulative traffic volume for a constant duration so that it is within the target range of values. Also, the proposed method works well using the simulation on a 1,000-user scale. We confirmed that the traffic volume can be controlled to a level lower than the upper bound for all evaluated conditions. Moreover, our method could control the traffic volume at 98.95% link usage against the target value. Therefore, we confirmed that this method is useful for a subscriber ISP that wants to control traffic from an upstream ISP in order to reduce the transit fee.

On the other hand, the traffic control system needs such information as content size provided by the application. We expect that cooperation between ISPs and ASPs is enabled by the framework being debated at IETF ALTO WG.

Acknowledgment

The authors wish to thank Dr. S. Akiba and Dr. Y. Nakajima of KDDI R&D Laboratories, Inc. for their guidance and constant encouragement. The authors also thank to Dr. M. Suzuki of KDDI R&D Laboratories, Inc. for his support of this study.

References

[1] Cisco Systems Inc., "Cisco Visual Networking Index: Forecast and Methodology, 2009-2014", http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html.
[2] BitTorrent, Inc., BitTorrent DNA, http://www.bittorrent.com/dna.
[3] Pando Web Page, http://www.pando.com/.
[4] A. Nakao, K. Sasaki, and S. Yamamoto, "A Remedy for Network Operators against Increasing P2P Traffic: Enabling Packet Cache for P2P Applications", IEICE Trans. on Communications, pp.3810-3820, 2008.
[5] C. Hsu, and M. Hefeeda, "ISP-Friendly Peer Matching without ISP Collaboration", Proc. Int. Workshop on ROADS'08, December 2008.
[6] H. Xie, Y. R. Yang, A. Krishnamurthy, Y. Liu, and A. Silberschatz, "P4P: Provider Portal for Applications", Proc. ACM SIGCOMM'08, pp.351-362, August 2008.
[7] M. Shibuya, T. Ogishi, and S. Yamamoto, "A Study on Traffic Localization Issue for P2P Content Delivery", Proc. IMSA 2009, pp.26-32, August 2009.
[8] MaxMind, Inc., GeoIP Web Page, http://www.maxmind.com/app/ip-location.
[9] http://www.bittorrent.org/beps/bep_0003.html.
[10] M. Shibuya, T. Ogishi, and T. Kato, "Evaluation of Content Delivery Characteristics using Network-aware P2P Simulator", IEICE technical Report, IN2009-155, pp.67-72, March 2010. (in Japanese)
[11] IETF ALTO WG, http://tools.ietf.org/wg/alto/.

Megumi Shibuya has joined KDD R&D Labs Inc. (currently KDDI R&D Labs Inc.) in 1994. From 1994 to 2002, her main activity was the research on the satellite resource management system for a non–GSO system. From 2003 to 2005, she was engaged in the research on optical signal space transmission technologies. She has been engaged in the research on P2P distributed content delivery in the broadband access network. She is working on Network Integration Lab. in KDDI R&D Labs Inc. She is now with the Graduate School of Information Network Systems, the University of Electro-Communications.

Tomohiko Ogishi received the B.E. degree in electrical engineering from the University of Tokyo in 1992 and the Ph.D. degree in engineering from the University of Electro-Communications in 2008, respectively. Since joining KDD in 1992, he has been working in the field of testing and monitoring of communication systems. He is currently the senior manager of Network Integration Lab. in KDDI R&D Labs Inc. He received the Young Engineer Award of IEICE in 1998.

Open Science Index, Computer and Information Engineering Vol:4, No:11, 2010 publications.waset.org/1121.pdf