

Analysis and Application of Passive Peer Influence on Peer-to-Peer Inter-domain Traffic

Atsushi TAGAMI, Teruyuki HASEGAWA and Toru HASEGAWA

KDDI R&D Laboratories Inc.

E-mail: tagami@kddilabs.jp

Abstract

As a result of widespread of Peer-to-Peer (P2P) file sharing applications, it is a serious problem that inter-domain traffic between Internet Service Provider (ISP) networks increases. In this paper, we present a novel inter-domain traffic flow model focusing on the presence of a passive peer, and proposes a new P2P traffic control method based on the model. This method uses a filter considering P2P flow characteristics and can be applied to the P2P networks whose protocol is closed. We also evaluate both validity and effectiveness of our proposals by performing more than 20 days experiments using real P2P network environment. The results prove that our model is reasonable enough and the proposed method is promising for decreasing inter-domain P2P traffic.

1. Introduction

Since Napster[1] appeared in 1999, various Peer-to-Peer (P2P) file sharing applications (e.g., WinMX, KaZaA, Gnutella, Freenet, winny) have emerged one after another. According to rapid spread of such applications, their traffic volume (we call it “P2P traffic”) has been explosively increasing and this trend is considered to be continued[2]. Reference [3] pointed out that P2P traffic had been already consuming the major part of bandwidth of the authors’ inter-domain links connecting to the other domains.

From the viewpoint of inter-domain traffic volume, P2P traffic has undesirable characteristics compared with traditional Web traffic. First, transmission object data size of P2P applications is huge. Reference [3] reported that median P2P object size is 4Mbytes. while median Web object size is 2Kbytes. Second, P2P traffic demand is not centralized in some locations, e.g., Data Centers, as server-client based Web applications, but is distributed uniformly into any pair of P2P terminals (peers) all over the Internet. In other words, P2P applications build symmetrical

overlay networks (we call it “P2P networks”) on physical networks[4], on which all peers communicate each other without considering their physical network locations. We consider these characteristics have a serious impact on inter-domain link bandwidth at first because it is relatively smaller and more difficult to extend than intra-domain one. Therefore, many Internet Service Providers (ISPs) need to control P2P traffic especially on inter-domain links.

There are several works on P2P traffic control[5, 6, 7, 8]. The most general methods adopted in commercial systems are based on P2P connection identification and restriction such as filtering or bandwidth limiting[5, 6]. However, the identification becomes more difficult today because of the following reasons.

- Today’s P2P applications such as Gnutella do not use any well-known TCP port numbers and any special IP destinations, i.e., TCP port number/IP address based identification is impossible.
- Some P2P applications use encrypted messages for resource discovery and transfer, i.e., P2P application level analysis is complex.
- The bandwidth of Internet access link is rapidly growing, i.e., online P2P identification requires enormous processing power.

The other methods are based on introducing some asymmetry into symmetrical P2P networks along physical network topology. For example, reference [7] proposed to deploy “Cache Servers” on their proprietary P2P networks in order to save redundant resource transfer. Reference [8] presented network-aware clustering techniques which help to construct P2P networks fitting to physical topology by restricting each peer to communicate with physically remote peers. However these approaches can be taken only in the case that P2P file sharing application protocol is disclosed and/or is possible to be modified. Practically, since the protocol is closed in some major P2P file sharing applications such as KaZaA and winny, it is also necessary for some method to control the P2P traffic even if its protocol is closed.

Based on the above background, we have proposed to use “*passive peer*” for providing resource cache equivalent functions on such protocol closed P2P networks[9]. The passive peer is realized by execution of corresponding P2P application without any change, but it does not perform any active operations such as resource creation and resource request (download request) origination, i.e., it only caches, relays and replies resources. In addition, some filtering function is introduced in order to limit outgoing traffic from the passive peer to other domains based on TCP connection level byte accounting to which P2P traffic characteristics is reflected. As a result, the passive peer behaves as a resource cache according to physical network topology and inter-domain P2P traffic is expected to decrease.

In order to deploy our method into ISPs, it is important to analyze the effectiveness of the proposed method theoretically based on a reasonable inter-domain traffic flow model of resource transfer. However recent works were mainly focusing on P2P network scale, e.g., analyzing the number of hops and search messages for finding/getting resources[10][11]. This paper presents a novel inter-domain traffic flow model considering the influence of additional passive peer, and gives some theoretical analysis on the method. Moreover we evaluate the validity of the model using captured traffic on a real P2P network.

The rest of paper is organized as follows. Section 2 describes a target P2P file sharing application and gives our inter-domain traffic flow model including our proposed method. Section 3 explains about winny, the most popular P2P file sharing application in Japan. Section 4 explains traffic capture environment for a winny network and discusses the validity of presented model. Section 5 discusses the implementation and effectiveness of proposed method based on statistical analysis of captured traffic. Section 6 gives some conclusions.

2. P2P Inter-domain Traffic Flow Model

2.1. P2P File Sharing Application Overviews

P2P file sharing applications are classified according to centralized server existence: hybrid and pure models[12]. In a hybrid model, a centralized server is used to store meta-information pieces such as identifiers and locations of resources. At first a peer sends a search query to the server to know the resource location as illustrated in Fig. 1. Then it downloads the resource from the peer whose location is replied by the server. In a pure model, a centralized server is not used for resource search. A search query is relayed on a hop-by-hop basis to the peer that knows the resource location. Examples of hybrid model include Napster, and examples of pure model include Gnutella, Freenet.

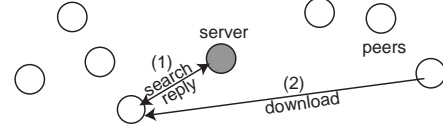


Figure 1: Hybrid Peer-to-Peer Model

Resource replication is widely used in pure P2P file sharing applications[13] to protect resources from disappearing due to peers leaving the P2P network. Figure 2 shows how a resource is replicated. The reply with the resource is relayed on a hop-by-hop basis from the peer holding the resource. Each peer on the relay path stores the copy of resource (replicates it). Even if the peer is passive, i.e., it does not originate any resource request, some resources are replicated.

In this paper we consider pure P2P file sharing applications with replication because pure models are becoming more popular than hybrid models, and because the replication is commonly used among such applications.

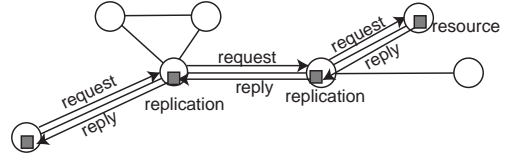


Figure 2: A Example of Replication

2.2. Traffic Flow Model

In this section we describe the traffic flow model, based on which we design a P2P traffic control method. As illustrated in Fig. 3, the model consists of two types of domains: My Domain and Other Domains. A domain represents a set of peers inside the same administrative scope. In typical cases, a domain is equivalent to an ISP network. A passive peer is added to the domain of interest, i.e., My Domain. This is used to control traffic between My Domain and Other Domains, i.e., to reduce inter-domain P2P traffic.

Traffic T is the total traffic amount both incoming to and outgoing from the passive peer since the passive peer was added. T is divided into four kinds of traffic $T_{out}^m, T_{out}^o, T_{in}^m, T_{in}^o$ according to the directions of T . 'out', 'in', 'm' and 'o' account for outgoing, incoming, My Domain and Other Domains, respectively. We define the direction from the passive peer to other peers as outgoing, and all the other direction as incoming. For example, T_{out}^m is the total traffic amount from the passive peer to peers in My Domain. T_{in}^o is that from peers in Other Domains to the passive peer.

Each peer selects destination peers for communication. Let p and q be the probabilities that a peer selects destina-

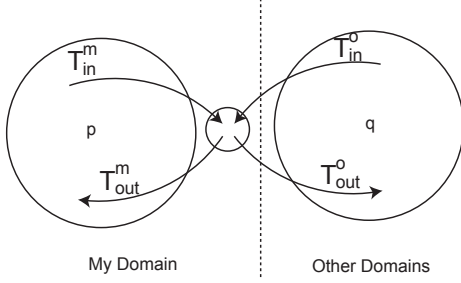


Figure 3: Traffic Flow Model

tion peers in My Domain and Other Domains, respectively (we call it “*selection probabilities*”). Note that $q = 1 - p$. We assume that p (and also q) is equal for all the peers. From this assumption, T_{in}^m , T_{out}^m , T_{in}^o and T_{out}^o satisfy the following equation:

$$\frac{T_{in}^m}{T_{out}^m} = \frac{T_{in}^o}{T_{out}^o} = \frac{p}{q} \quad (p \neq 0, q \neq 0) \quad (1)$$

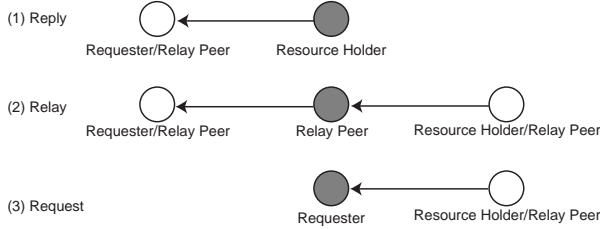


Figure 4: Three Roles of P2P Peer in Resource Transfer

Figure 4 depicts how a peer behaves when a resource request is received. A peer can play the following 3 roles: Resource Holder, Relay Peer and Requester. If a peer holds the requested resource, it works as Resource Holder which replies a stored resource to the requesting peer. The requesting peer is either Requester or Relay Peer. If a peer does not hold the resource, it works as Relay Peer which forwards this request to another peer, and wait for reply. Then it relays the resource reply to the requesting peer. However note that a passive peer does not originate any resource request. In other words, a passive peer does not work as Requester. Therefore, the model deals with only the reply and relay traffic considering that the passive peer works as either Resource Holder or Relay Peer.

Since the passive peer doesn't create any new resources, all resources of the passive peer are received from others. The passive peer works as a resources cache and the cache performance κ is defined as:

$$\kappa = \frac{T_{out}}{T_{in}} \quad (2)$$

where T_{out} and T_{in} are defined as:

$$\begin{cases} T_{out} = T_{out}^m + T_{out}^o \\ T_{in} = T_{in}^m + T_{in}^o \end{cases}$$

2.3. Traffic Flow Change

In this section we discuss the inter-domain traffic flow change caused by the addition of passive peer. First, let \mathfrak{I}_{peer} be the total amount of inter-domain traffic in the case that a passive peer is added. \mathfrak{I}_{peer} is defined by the following equation:

$$\mathfrak{I}_{peer} = T_{in}^o + T_{out}^o \quad (3)$$

Second, we define the inter-domain traffic without the addition of passive peer. If the passive peer were not added:

- T_{in}^m and T_{in}^o were disappeared because the passive peer does not originate any resource request, and
- resources transferred from/via the passive peer, i.e., T_{out}^m and T_{out}^o , would be directly transferred from other peers (we call them “*alternative peers*”) as shown in Fig. 5.

Thus we can regard T_{out}^m and T_{out}^o ($= T_{out}$) as inherent resource transfer demands among four types of traffic flow in Fig. 3, irrespective of the presence of passive peer. Since alternative peers are selected randomly, they are divided into those in My Domain and Other Domains according to the selection probability p and q . Figure 6 shows how T_{out}^m and T_{out}^o migrates to the alternative peers. For example, T_{out}^m is divided into pT_{out}^m and qT_{out}^m , the former is intra-domain and the latter is inter-domain traffic respectively. T_{out}^o , T_{out}^m , p and q satisfy the following equation:

$$\begin{cases} T_{out}^o = pT_{out}^o + qT_{out}^m \\ T_{out}^m = pT_{out}^m + qT_{out}^m \end{cases} \quad (4)$$

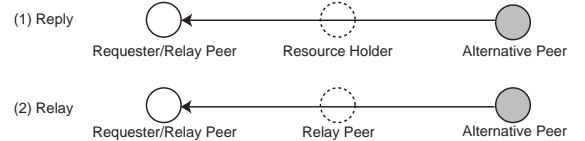


Figure 5: P2P Peer Behaviors in Resources Transfer without Passive Peer

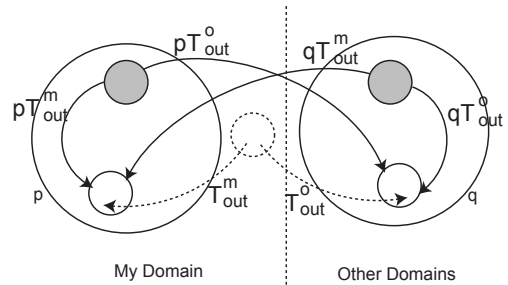


Figure 6: Traffic Flows without Passive Peer

Let $\mathfrak{I}_{nonpeer}$ be the total amount of inter-domain traffic without the passive peer. $\mathfrak{I}_{nonpeer}$ is defined by following equation:

$$\mathfrak{I}_{nonpeer} = qT_{out}^m + pT_{out}^o \quad (5)$$

The traffic amount flow change caused by the passive peer is the difference between $\mathfrak{I}_{nonpeer}$ and \mathfrak{I}_{peer} . Let r be the ratio of $\mathfrak{I}_{nonpeer}$ to \mathfrak{I}_{peer} . In order to decrease inter-domain traffic decrease by adding the the passive peer, the following inequality must be satisfied:

$$r < 1 \quad (6)$$

Otherwise, the inter-domain traffic increase adversely.

We obtain the condition that the inter-domain traffic decreases in the following way. Using equation (3) and (5) we get:

$$\begin{aligned} r &= \frac{\mathfrak{I}_{peer}}{\mathfrak{I}_{nonpeer}} \\ &= \frac{T_{in}^o + T_{out}^o}{qT_{out}^m + pT_{out}^o} \\ &= \frac{1 + T_{out}^o/T_{in}^o}{qT_{out}^m/T_{in}^o + pT_{out}^o/T_{in}^o} \end{aligned} \quad (7)$$

Substitute equation (1) and (2) for equation (7):

$$r = \frac{1 + \kappa}{2p\kappa} \quad (8)$$

Substitute for equation (6)

$$\frac{\kappa + 1}{2p\kappa} < 1$$

Solving this inequality for κ subject to $0 < p < 1$ and $\kappa > 0$:

$$\kappa > \frac{1}{2p - 1} \quad (p > \frac{1}{2}) \quad (9)$$

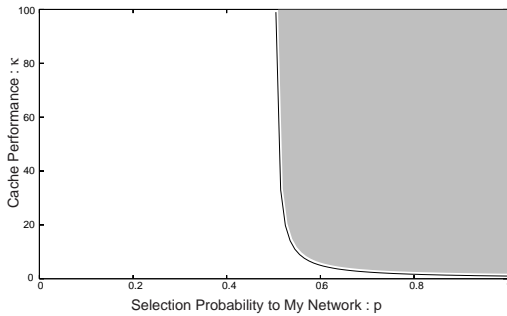


Figure 7: Area of Decrease Inter-domain Traffic by Passive Peer

The shaded part in Fig. 7 indicates the area satisfying inequality (9), in which the passive peer can reduce inter-domain traffic. It is clear that if the selection probability to

My Domain p is less than $1/2$, the inter-domain traffic always increases due to the passive peer. On the contrary, the probability must be at least $1/2$ to decrease the inter-domain traffic.

2.4. Proposed Method

We assume that the passive peer is added to an ISP network. Because the ISP network corresponds to My Domain, it is unlikely that the connection probability p is greater than $1/2$. Since the passive peer addition itself does not decrease the inter-domain traffic, we propose a method to decrease the inter-domain traffic by controlling traffic flow of the passive peer[9].

In order to decrease the inter-domain traffic, T_{in}^o and/or T_{out}^o need be suppressed. However, if T_{in}^o is suppressed, the passive peer cannot receive and store (for replication) resources. This reduces cache performance κ of the passive peer. From equation (8), it is clear that the decrease of κ leads to the increase of r . Since we cannot limit T_{in}^o , we restrict T_{out}^o which is the traffic flow outgoing from the passive peer.

In the rest of section, we consider the passive peer with the filtering limitation for T_{out}^o . Let $T_{out}^{'o}$ be the traffic amount after the traffic limitation, and δ be the limit ratio. $T_{out}^{'o}$, T_{out}^o and δ satisfy the following equation:

$$T_{out}^{'o} = \delta T_{out}^o \quad (0 < \delta < 1) \quad (10)$$

The above limitation reduces the inter-domain traffic to $T_{out}^o - T_{out}^{'o}$. However a peer whose resource transfer is filtered (we call it *filtered peer*) tries to get it from another peer. Some of the limited traffic again becomes the inter-domain traffic because some peers in My Domain is chosen by the filtered peer in Other Domains. Let \mathfrak{I}_{peer-f} be the inter-domain traffic in the case that the passive peer with such traffic limitation is added to My Domain. Since the peer is chosen according to selection probability p , \mathfrak{I}_{peer-f} is defined by the following equation:

$$\begin{aligned} \mathfrak{I}_{peer-f} &= (T_{in}^o + T_{out}^{'o}) + p(T_{out}^o - T_{out}^{'o}) \\ &= T_{in}^o + (p + q\delta)T_{out}^o \end{aligned} \quad (11)$$

Rewriting equation (7) using (11), we can obtain r_f , the ratio r with the limitation:

$$\begin{aligned} r_f &= \frac{\mathfrak{I}_{peer-f}}{\mathfrak{I}_{nonpeer}} \\ &= \frac{T_{in}^o + (p + q\delta)T_{out}^o}{qT_{out}^m + pT_{out}^o} \\ &= \frac{1 + (p + q\delta)\kappa}{2p\kappa} \end{aligned} \quad (12)$$

In order to decrease the inter-domain traffic, the following inequality must be satisfied:

$$r_f < 1$$

$$\frac{\kappa(p + q\delta) + 1}{2p\kappa} < 1$$

We finally obtain the following inequality for κ subject to $0 < p < 1$ and $\kappa > 0$:

$$\kappa > \frac{1}{p - q\delta} \quad (p > \frac{\delta}{\delta + 1}) \quad (13)$$

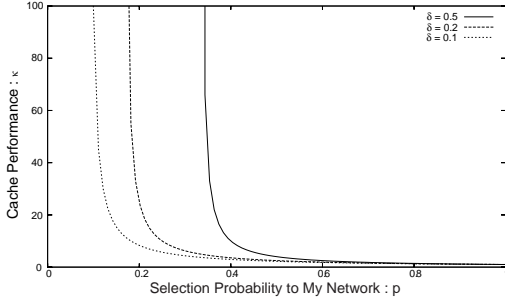


Figure 8: Effective Area in Proposal Method

Figure 8 shows the effective areas for several δ values (0.5, 0.2 and 0.1) in the proposed method. This figure makes it clear that the smaller δ becomes, the lesser the inter-domain traffic becomes, even if the selection probability p is less than 1/2.

2.5. Time Dependency

Up to here, we have discussed the total traffic amount since the passive peer was added. In this section we extend the discussion to the transition of traffic amount change. We define time series traffic data each of which represents a value of some time period (e.g., 24 hours). Let $\mathfrak{I}_{nonpeer}(t)$ and $\mathfrak{I}_{peer}(t)$ be the inter-domain traffic without the passive peer at the t th period ($t = 1, 2, 3 \dots$), and that with the peer at t th period, respectively. $\mathfrak{I}_{nonpeer}(t)$ and $\mathfrak{I}_{peer}(t)$ are defined by the following equations:

$$\begin{aligned} \mathfrak{I}_{nonpeer}(t) &= qT_{out}^m(t) + pT_{out}^o(t) \\ \mathfrak{I}_{peer}(t) &= T_{in}^o(t) + T_{out}^o(t) \end{aligned}$$

Cache performance of passive peer at the t th period $\kappa(t)$ is defined by the following equation:

$$\kappa(t) = \frac{T_{out}(t)}{T_{in}(t)} \quad (14)$$

Let $r(t)$ be the rate of $\mathfrak{I}_{nonpeer}(t)$ to $\mathfrak{I}_{peer}(t)$. $r(t)$ represents the traffic amount change due to the passive peer at the t th period. we get:

$$\begin{aligned} r(t) &= \frac{\mathfrak{I}_{peer}(t)}{\mathfrak{I}_{nonpeer}(t)} \\ &= \frac{1 + \kappa(t)}{2p\kappa(t)} \end{aligned} \quad (15)$$

Let $r_f(t)$ be the rate of $\mathfrak{I}_{nonpeer}(t)$ to $\mathfrak{I}_{peer-f}(t)$ considering the limitation in the passive peer. $r_f(t)$ is expressed as:

$$r_f(t) = \frac{1 + (p + q\delta)\kappa(t)}{2p\kappa(t)} \quad (16)$$

$T_{out}(t)$, which is traffic flow outgoing from the passive peer in t th time period, is the sum of the relay traffic from other peers and the reply traffic using its own stored resources. The reply traffic is considered to increase corresponding to the volume of stored resources. In other words, if the volume of stored resources becomes large, the passive peer is likely to send a stored resource instead of relaying the resource from another peer. We assume that the stored resource volume continuously increases as time goes by if the passive peer is equipped with an enough storage. If this assumption is correct, $T_{out}(t)$, which includes the reply traffic, increases with t . Thus, $\kappa(t)$ increases with t (See equation (14)). Finally, as shown in Fig. 8, $r_f(t)$ decreases with t . This means that the proposed method is expected to decrease further the inter-domain traffic as time goes by.

3. P2P File Sharing Application

We chose winny which is one of pure P2P file sharing applications. Winny has been used popularly since 2002 in Japan. The winny protocol is kept proprietary, and there is no official technical document on how a winny peer works. According to some public information [15], the winny design follows the Freenet architecture. Winny has following features:

- encrypted messages and anonymity mechanisms for resources and users,
- node hash keys which are computed from IP address and TCP port number,
- resource replication using some pretending technique for protection from leaving peers,
- dynamic P2P overlay network optimization, and
- separation of a resource transfer from a search, i.e., the resource is directly transferred from a peer found by a search request, which is different from Freenet.

Fig. 9 shows how a resource is searched and transferred over a winny network. We explain an example communication sequence of winny according to Fig. 9.

1. A resource holder (peer f), i.e., a peer which has some resource, distributes a key to neighbor peers. The key includes some meta-information about the resource and its holder.
2. A peer forwards a received key to another peer periodically, e.g., every one second, so that the key is flooded to many peers. The peer (peer d) changes frequently

a resource holder entry on the key from the current holder to itself in order to pretend the resource holder.

3. A requester (peer a) sends a search query to neighbor peer, and receives the reply which includes the corresponding key.
4. A requester then sends resource request to the resource holder according to the key. The holder is sometime a pretending holder (peer d). Since the pretending holder does not hold the resource, it send the resource request to the next resource holder (peer f: actual holder). Then the pretending holder receives the resource, replicates it and relays it to the requester.

In Fig. 9, peer d replaces a resource holder entry on a key created by peer f to itself. A requested resource is transferred on $f \rightarrow d \rightarrow a$, and is replicated by peers d and a.

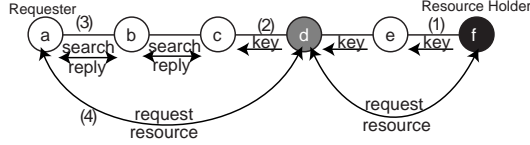


Figure 9: Searching and Transferring Resource over Winny Network

This behavior of replication, where resources are replicated by all peers on the resource transfer path, is called Path Replication[13]. However, the resource transfer path is not the same as the search path in winny although those are the same in Freenet.

4. Validity of Traffic Flow Model

4.1. Traffic Measurement

In order to evaluate the validity of the traffic flow model described in section 2, we installed a passive peer in an ISP network and captured traffic between the passive peer and winny peers all over the Internet. Figure 10 shows the traffic measurement environment. A PC (P2P Passive Peer) on which winny runs is connected to an ISP network through a 100 Mbps access line. The P2P peer doesn't create any resource and doesn't originate any resource request so that it works just as a passive peer. The ISP network consists of 46 subnets, and has about 2 million IP addresses including network and broadcast addresses. Table 1 shows the specification of PC for P2P passive peer. We ran this P2P passive peer for 21 days, and captured all the winny traffic outgoing from and incoming to it.

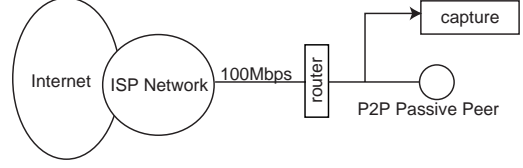


Figure 10: Traffic Measurement Environment

4.2. Selection Probability

First, we analyze the captured traffic to verify equation (1). Table 2 shows the summary of the captured traffic. As shown in Fig.3, total amount of captured traffic T is divided into four kinds: T_{out}^m , T_{out}^o , T_{in}^m and T_{in}^o . We calculate the selection probability p and q independently from the outgoing traffic (T_{out}^m/T_{out}^o) and the incoming traffic (T_{in}^m/T_{in}^o) according to equation (1). The results are shown in table 2. The ratio of q to p is similar in the case of the outgoing traffic and the incoming traffic. We consider that this small difference is owing to the correctness of equation (1).

We then plots the change of selection probability p on Fig. 11 when target duration of calculation is increased. Each plot represent a value calculated from the traffic whose capture duration is the day of x-axis. For example, a value of p at the 5th day is calculated from the total traffic for 5 days. We consider that the selection probability gradually converges. But unfortunately, 21 days are not long enough to verify the convergence.

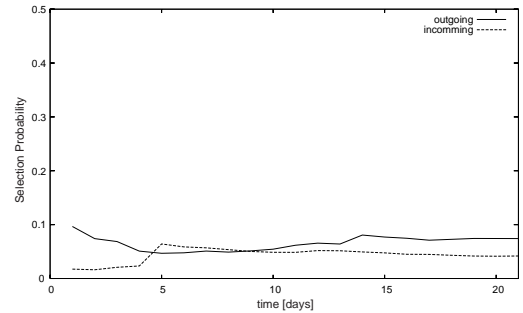


Figure 11: Change of Selection Probability

4.3. Cache Performances

Figure 12 shows the transition of cache performance of the passive peer until 21th day, i.e., $\kappa(t)$ ($t = 1, 2, \dots, 21$). Each $\kappa(t)$ value is calculated using 1 day traffic on the t th

Table 1: Specification of PC for P2P Passive Peer

CPU	Pentium III 750MHz
Memory	256MB
OS	Windows 2000 SP4
Shared disk	1.6TB
P2P Application	winny 2.0β7.1

Table 2: Summary of Measured Traffic

	outgoing	incoming
My Domain	25,737 MB	875 MB
Other Domains	321,241 MB	20,049 MB
p	0.075176	0.041843
q	0.925824	0.958157

day. It is clear that $\kappa(t)$ increases continuously as long-term tendency, and this confirms the assumption described in section 2.5. Therefore we consider that $r_f(t)$ may decrease as the time goes by, i.e., the inter-domain traffic decreases.

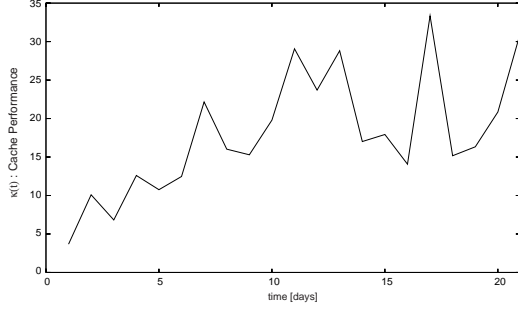


Figure 12: $\kappa(t)$: Cache Performance of Passive Peer

5. Implementation and Effectiveness

5.1. Implementation of Proposed Method

As described in section 2.4, the proposed method limits the amount of outgoing traffic from a passive peer. However, the method assumes that parameters such as p, q , which depend on P2P network topology, do not change due to the traffic limitation. Thus, we consider that the number of TCP connections limited by filter should remain as few as possible. In order to design good filtering policy, we classify TCP connections according to resource transfer amount. Figure 13 shows the relatively cumulative frequency about total connection number and total traffic amount. X-axis shows the byte amount of user data transferred on a connection. We can easily find that connections with over 5 Mbytes transfer occupy less than 1% of total connection number but occupy about 90% of total traffic amount. Therefore we design the filter so as to cut these connections.

Then we implement a filter that runs together with a P2P passive peer as shown in Fig. 14. The filter need not identify the P2P traffic because only P2P traffic passes through the filter. The filter cuts a TCP connection if:

- its destination peer is located on Other Domains, and
- cumulative outgoing data amount exceeds 5 Mbytes.

All IP addresses of My Domain are registered in advance on the filter so that the filter can identify connections to

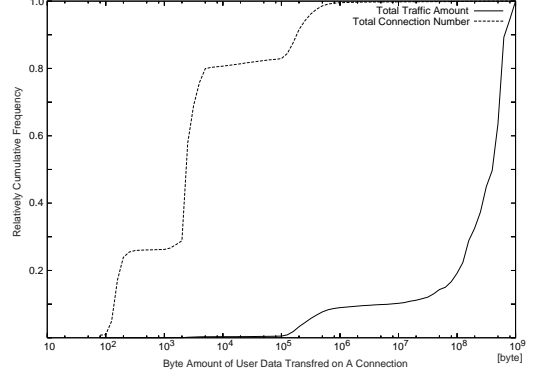


Figure 13: Relatively Cumulative Frequency about Total Connection Number and Total Traffic Amount

Other Domains. Besides, since a peer of the filtered connection tries to the P2P passive peer again, the filter also blocks the following connections:

- new TCP connection from a peer of filtered connection within 30 sec.

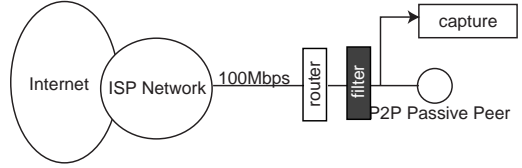


Figure 14: Implementation of Proposal Method and Traffic Measurement Environment

Hereafter we give some discussion about our implementation using the measurement results.

5.2. Validity of Implementation

First we discuss the validity of the implementation. Equation (1) requests that the selection probability p is equal for every peer. On the other hand, the filter cuts some of the TCP connections, so that the P2P passive peer may seem unstable to other peers. If other peers avoided connecting with the P2P passive peer, the corresponding traffic, with which the P2P passive peer would deal, would disappear. Therefore we analyze the captured traffic to estimate such side effects of the filtering.

Our implementation cuts TCP connections whose data transfer direction is outgoing from the passive peer to peers in Other domains, which corresponds to T_{out}^o . If T_{out}^o decreased while T_m^o was unchanged, T_{out}^m/T_{out}^o would be changed and equation (1) would be inconsistent. Although T_{out}^o must be known for observing the change of T_{out}^m/T_{out}^o , we can only measure T_{out}^{io} instead. There-

fore we consider the change of number of TCP connections as substitutes for T_{out}^m/T_{out}^o .

We classify the connections into four groups according to a couple of viewpoints: the ratio of outgoing traffic amount to incoming and the Domain type of destination peers. Let $C_{in}^m, C_{out}^m, C_{in}^o$ and C_{out}^o be the numbers of connections of the four groups. For example, C_{in}^m is the number of connections of which incoming traffic amount is larger than outgoing, and of which destination peers are in My Domain. We consider that C_{in}^m/C_{in}^o and C_{out}^m/C_{out}^o substitute for T_{in}^m/T_{in}^o and T_{out}^m/T_{out}^o . Figure 15 and Table 3 show the selection probability p calculated from $C_{in}^m/C_{in}^o, C_{out}^m/C_{out}^o$ in the basis of day and the total days, respectively.

As shown in Table 3, the ratio of q to p is similar in both outgoing and incoming connection cases. In addition, Fig. 15 indicates the selection probability values are almost stable in any time scale, i.e., 1 day through 30 days calculation duration. Therefore, we conclude that the outgoing connection cutting does not affect the selection probability p .

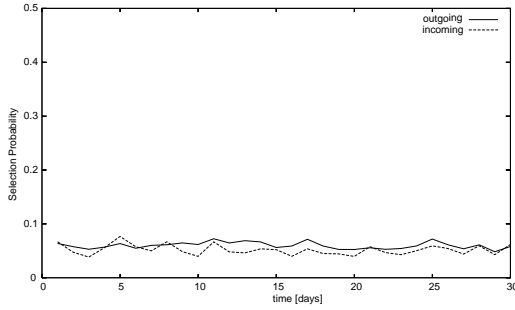


Figure 15: Selection Probability Calculated from Number of Connections

Table 3: Summary of Selection Probability Calculated from Number of Connections

	outgoing	incoming
p	0.059875	0.05185
σ^2	$3.9 * 10^{-5}$	$9.1 * 10^{-5}$

5.3. Effectiveness of Proposed Method

Second we discuss how the proposed method decreases the inter-domain traffic. We calculate the inherent mount of the outgoing traffic to Other Domains on the basis of day, i.e., $T_{out}^o(t)$, that would be transferred to Other Domains if the traffic were not limited. Since we cannot measure the inherent outgoing traffic, we obtain $T_{out}^o(t)$ using equation (1) as follows:

$$T_{out}^o(t) = \frac{T_{out}^m(t)T_{in}^o(t)}{T_{in}^m(t)} \quad (17)$$

We also calculate limit ratio $\delta(t)$ from $T_{in}^o(t)$ and $T_{out}^o(t)$. $T_{out}^o(t)$ is calculated by equation (17), and $T_{in}^o(t)$ is decided based on the analysis of captured traffic. Figure 16 shows the limit ratio $\delta(t)$ is almost between 0.01 and 0.05 except for several days.

In addition, we calculate $r_f(t)$, the ratio of the traffic amount without the passive peer to that with the passive peer and the filter, for several possible pairs of limit ratio $\delta(t)$ and selection probability p . 0.01 and 0.05 are chosen as $\delta(t)$, and 0.059875 and 0.05185 shown in Table 12 are chosen as p . Figure 17 plots ratio $r_f(t)$ to cache performance $\kappa(t)$ of the x-axis. This graph shows that if $\kappa(t)$ is large enough, the inter-domain traffic can be decreased (i.e. $r_f(t) < 1$) by our method even if p is only around 5% such as our measurement environment.

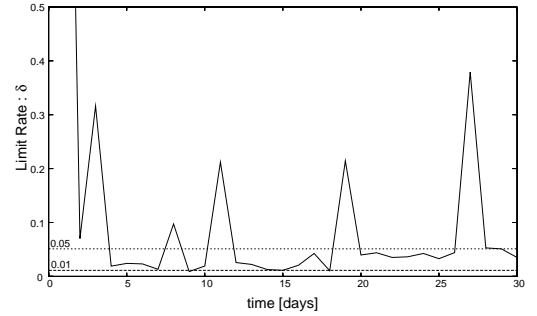


Figure 16: Limit Rate : $\delta(t)$

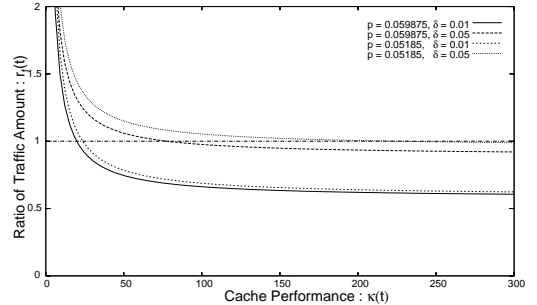


Figure 17: Rate of Inter-Domain Traffic Change

Finally, we calculate $r_f(t)$ on the basis of day according to equation (5) and plot on Fig. 18. Figure 18 shows $r_f(t)$ gradually decreases and becomes less than 1 at 12th day. After the day, $r_f(t)$ is almost always less than 1, and its values are about 0.55 to 0.98. This means the proposed method can decrease about 2-45% of $\mathfrak{I}_{nonpeer}$. We conclude that, at our experiment, the proposed method successfully decreases the daily inter-domain traffic after 12th day without a few exceptions, and that it is expected to decrease the inter-domain traffic after that.

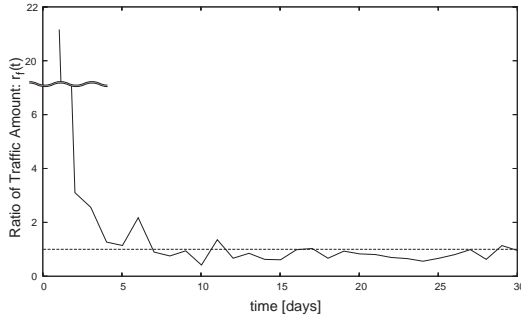


Figure 18: Rate of Inter-domain Traffic Change by Passive Peer

6. Conclusion

In this paper, we discuss a novel traffic flow model of P2P file sharing application, which aims to grasp inter-domain P2P traffic trend. This model has the following features.

- The “*passive peer*” concepts, where we operate a P2P peer itself as a resource cache, are adopted in order to give some influence on inter-domain P2P traffic even if its protocol details are not disclosed.
- The traffic related to the passive peer is classified into four types according to traffic directions (incoming/outgoing) and the physical locations of destination peers (My Domain/Other Domains).
- As for the peer selection behavior, we assume that all the peers select peers in My Domain following the same probability p .
- Traffic limitation for traffic T_{out}^o (outgoing and Other Domains) is also considered in order to give positive influence on inter-domain P2P traffic.

Using the model, we show the passive peer itself cannot decrease inter-domain P2P traffic, rather increase it in the case of $p < 1/2$. But we prove that inter-domain traffic can be decreased even in the case of $p < 1/2$ by applying traffic limitation of T_{out}^o , the traffic outgoing from the passive peer to peers in Other Domains. We also indicates that the decreasing ratio is improved as time goes by.

Next we measure real traffic of “*winny*” which is the most popular P2P file sharing application in Japan. From this measurement result, we find the uniformity of selection probability p is maintained within 0.05 (5%) accuracy, so that the validity of the model is cleared.

Moreover, we design and implement a simple filtering method of T_{out}^o considering winny traffic characteristics. We also introduce our filter implementation and a passive peer into an ISP network with about 2 million IP addresses, and evaluate the proposed method. According to this evaluation result, we can conclude that the proposed method can decrease about 2-45% traffic between ISP Networks.

References

- [1] The Napster home page, <http://www.napster.com/>.
- [2] Satoshi Kamei, Tatsuya Mori, Keita Ooi, “Status and Traffic Issues of Peer-to-Peer File Sharing Applications — for traffic measurement, traffic control, network design, and operation,” Technical Report of IEICE, CQ2003-40, Sep. 2003. (in Japanese)
- [3] Stefan Saroiu, Krishna P. Gummadi, Richard J. Dunn, Steven D. Gribble, Henry M. Levy, “An Analysis of Internet Content Delivery Systems,” Proc. of the 5th Symposium on Operating Systems Design and Implementation, Boston, MA, Dec. 2002.
- [4] Demetris Zeinalipour-Yazti and Theodoros Folias, “A Quantitative Analysis of the Gnutella Network Traffic”, Unpublished, April 2002.
- [5] P-Cube Inc, “Approaches To Controlling Peer-to-Peer Traffic,” Technical White Paper, <http://www.p-cube.com/>.
- [6] Ellacoya Networks, <http://www.ellacoya.com/>.
- [7] Tetsuya Oh-ishi, Koji Sakai, Tetsuya Iwata and Akira Kurokawa, “The Deployment of Cache Servers in P2P Networks for Improved Performance in Content-Delivery,” Proc. of the Third International Conference on Peer-to-Peer Computing, Linköping, pp.22-29, Sweden, Sep. 2003.
- [8] Balachander Krishnamurthy, Jia Eang, Yinglian Xie, “Early Measurements of a Cluster-based Architecture for P2P Systems,” ACM SIGCOMM Internet Measurement Workshop, SF, Nov. 2001.
- [9] Atsushi Tagami, Julian Carbonell, Teruyuki Hasegawa, Toru Hasegawa, “A Peer-to-Peer Traffic Control Method with TCP Flow Analysis,” Proc. of the 66th National Convention of IPSJ, Mar. 2004. (in Japanese)
- [10] Krishna Kant, “An Analytic Model for Peer to Peer File Sharing Networks,” Proc. of International Communications Conference, Anchorage, AL, May 2003.
- [11] Mihajlo A. Jovanovic, Fred S. Annexstein and Kenneth A. Berman, “Scalability Issues in Large Peer-to-Peer Networks - A Case Study of Gnutella”, University of Cincinnati Technical Report 2001.
- [12] Dekan S. Milojević, Vana Kalogeraki, Rajan Lkose, Kiran Nagaraja, Jim Pruyne, Brund Richardm, Sami Rollins and Zhichen Xu, “Peer-to-Peer Computing,” HP Labs Tech Report, HPL-2002-57, Mar. 2002.
- [13] Qin Lv, Pei Cao, Edith Cohen, Kai Li and Scott Shenker, “Search and Replication in Unstructured Peer-to-Peer Networks,” Proc. of ACM ICS, pp. 84-95, New York, June 2002.
- [14] Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong, “Freenet: A Distributed Anonymous Information Storage and Retrieval System,” In Proc. of the ICSI Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, July 2000.
- [15] winny.info, <http://winny.info/>. (in Japanese)