

TCP フロー解析に基づく P2P トラフィック制御手法の提案

田上 敦士[†]Julian Carbonell[‡]長谷川 輝之[†]長谷川 亨[†](株)KDDI 研究所[†]ENST[‡]

1. はじめに

ファイル共有型の P2P (Peer-To-Peer) アプリケーションは Napster が 1999 年に公開されて以後爆発的に普及し、様々なアプリケーションが開発されてきた。P2P アプリケーションによるトラフィック (P2P トラフィック) は、ブロードバンドアクセスの普及に伴い増加しており、今後もその傾向が続く事が予想される[1]。特に近年、ISP (Internet Service Provider) 間での P2P トラフィック増加が深刻化しており、P2P トラフィックの制御が重要な課題となっている。

既存の P2P トラフィックの制御手法として、P2P フローを検出し遮断もしくは帯域制御する手法が存在する[2]。しかしながら、本手法には匿名性を重視する P2P アプリケーションによる回避や、複雑なパケット処理によるスケーラビリティ欠如等、多くの問題がある。

そこで本稿では、P2P フローの特性を計測・解析し、その結果に基づき P2P トラフィックを制御する手法を提案する。

2. 既存技術

2.1 ファイル共有型 P2P アプリケーション

ファイル共有型 P2P アプリケーションは、各参加ユーザが持つファイルを検索するシステムと、検索により各ユーザが発見したファイルを直接、あるいは中継ノードを介して間接的に取得するシステムからなる。また大別して Napstar や WinMX 等の中央サーバを用いて検索を行なうハイブリッド型と、Gnutella や winny 等の中央サーバを持たないピア型に分類される。後者では、検索やファイル配布に P2P アプリケーションの動作するノード (P2P ノード) 間で構築された 論理的な P2P ネットワークを使用する。P2P ネットワークはアクセス回線帯域や CPU 速度など P2P ノードのプロファイルやノード間ファイル転送の成功率などの情報を元に各 P2P ノードが自律分散的に構築し、その構成は逐次動的に変化する。この為、必ずしも実ネットワークの構成とは適合せず、ネットワークに冗長なトラフィックが流れる。

2.2 P2P トラフィック制御手法

既存の P2P トラフィック制御手法として、TCP ポート番号やアプリケーションレベルでの解析等により P2P フローを検出しその帯域を制御する手法が存在する。しかし前者については P2P ノード毎のランダムな TCP ポート番号の使用や、特定の中央サーバを用いないピア型の普及により、検出が困難となっている。一方後者では、パケットのペイロードやプロトコルを解析し識別する手法が取られている。しかしながら大量のパケット処理によるスケーラビリティ

A Peer-to-Peer Traffic Control Method with TCP Flow Analysis.

Atsushi TAGAMI[†], Jukian CARBONELL[‡], Teruyuki HASEGAWA[†], Toru HASEGAWA[†]

[†] (株) KDDI 研究所, KDD R&D Laboratories, Inc.

[‡] ENST, école nationale supérieure des télécommunications.

の欠如や、ペイロードの暗号化、プロトコル毎の対応が必要であるという問題が存在する。

3. P2P トラフィック解析と制御手法の提案

前述の問題を解決する為に、実際の P2P ネットワーク上に流れるトラフィックを収集/解析し、P2P トラフィックの特性を調べた。さらに、その結果を元に P2P トラフィックの制御手法を検討した。

3.1 P2P トラフィック計測

日本国内で代表的なピア型 P2P アプリケーションである winny を対象とし、P2P トラフィックの計測を行なった。winny は Freenet をベースとしており、分割ダウンロードや、中継ノードを用いたダウンロードなど次世代 P2P ファイル共有アプリケーションと呼ばれるアプリケーションの機能を一通り有している。アクセス回線としては 100Mbps の回線を使用し、Firewall で winny が使用する port 番号以外のコネクションをフィルタリングした。winny 起動後は能動的なファイル検索/取得はせず、中継ノードとしてのみ動作させた。表 1 に 2003 年 11 月 15 日から 19 日までの 5 日間、フロー毎に転送データ量と接続時間を収集した結果を示す。

表 1: 収集結果

	11/15	11/16	11/17	11/18	11/19
フロー数	35120	36430	33839	36372	37287
データ量 (Gbyte)	21.23	24.12	26.48	25.33	27.55

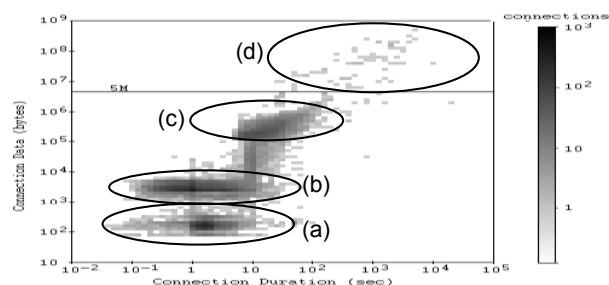


図 1: 転送データ量と接続時間によるフローの分布

図 1 に 11 月 19 日のデータを用いた転送データ量と接続時間に対するフローの分布を示す。この分布より P2P フローは転送データ量から (a) ~ (d) の大きく 4 つに分類できる。(a) ~ (d) それぞれの範囲におけるフロー数と転送データ量の合計を集計した結果を表 2 に示す。(a), (b) に分類されるフロー数は全体の 80% 以上であるが総転送データ量は 1% 未満であり、(d) に分類されるフロー数は逆に 1% 程度であるが総転送データ量は 74% を占める事がわかる。すなわち P2P トラフィックの制御は、(d) に分類されるフローを対象とする事が効果的であると言える。

表 2：フロー数による解析結果

	フロー数	総転送データ量 (Mbyte)
(a) (-1k)	9627 (25.7%)	1.88 (0.02%)
(b) (1k-10k)	20476 (54.6%)	68.80 (0.8%)
(c) (100k-2M)	6060 (16.2%)	1940.69 (23.7%)
(d) (5M-)	386 (1.0%)	6050.36 (74.0%)

次に 11 月 19 日のフローを以下の条件で upload, download, otherwise の 3 種類に分類した(表 3).

- upload：送信データ量が受信データ量の 2 倍より大きい場合
- download：送信データ量が受信データ量の 2 倍より大きい場合
- otherwise：上記区分に含まれない場合

表 3 より upload は download の 4 倍以上の総転送データ量がある事がわかる。これは P2P ノード自身が優良なファイルキャッシュとして動作している事を意味する。

表 3：データ転送方向による解析結果

	フロー数	総転送データ量(Mbyte)
upload	5976	6151.975
download	2518	1475.251
otherwise	29013	551.550

最後に 5 日分のデータを用いて、転送データ量を接続先ドメイン毎に集計した(表 4)。収集に用いた P2P ノードと同一ドメインに閉じたフローを内部ネットワークとの通信、それ以外を外部ネットワークとの通信とした(図 2)。表 4 より、大部分のトラヒックは ISP 間トラヒックとなる外部ネットワークとの通信である事がわかる。

表 4：接続先ドメインによる解析結果

接続先	受信	送信
外部ネットワーク	(1) 11.9Gbyte	(2) 79.5Gbyte
内部ネットワーク	(3) 0.43Gbyte	(4) 8.0Gbyte

3.2 提案手法

以上の結果より、P2P の TCP トラヒック特性に着眼した P2P トラヒック制御手法を提案する。本制御手法の目的はネットワーク間のトラヒックを軽減させる事である。まず、図 2 のように、P2P ノードに流れるトラヒックを接続相手(内部ネットワーク/外部ネットワーク)と転送方向で 4 つに分類する。前述のように P2P ノードは優良なキャッシュとして動作するので、送信データ量 ((2) + (4)) は受信データ量 ((1) + (3)) よりも大きい。しかしながら、外部ネットワーク向けの転送データ量が多いため ((1)+(2) > (3)+(4))、内部ネットワークに対する有効なキャッシュとは言えない。P2P ノードを内部ネットワークに対するキャッシュとして動作させる為には(2)の帯域を制限する事が有効である。しかしながら、(2)方向のトラヒックをすべて遮断した場合、外部ネットワークへの検索要求や応答が不可能となる。このため、しきい値を設定し特定のフローのみを遮断する事とした。具体的には、図 1、表 2 より(d)の領域のフローを遮断し、わずかなフローを制御する事でネットワーク間の P2P トラヒックの大幅な抑制を図った。

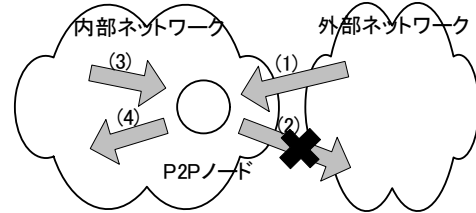


図 2：P2P ノードに流れるトラヒック

トラヒック制御装置は、制御対象の P2P アプリケーションが動作する P2P ノードと、収集装置ならびにフィルタ装置からなる。P2P ノードは一般ユーザが使用する P2P アプリケーションをそのまま起動し、P2P トラヒックを引き込む。収集装置は P2P ノードの送受信するトラヒックを収集し、フロー毎に転送データ量を記録する。フローは通常、送受信 IP アドレス/PORT 番号の 4 つ組で識別するが、P2P ノード側の IP アドレス/PORT 番号は固定であるため、接続先の IP アドレス/PORT 番号の組で識別する。ネットワークの内部/外部の識別は、内部ネットワークの IP アドレス一覧により行なう。P2P ノードから送信方向の転送データがしきい値を超えた場合、フィルタ装置にそのフローに対する RESET パケット送信を指示する。さらにフィルタ装置は同一 P2P ノードからの再接続を一定時間遮断する。

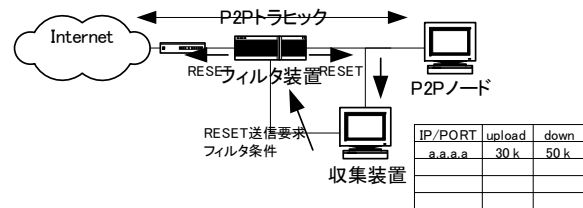


図 3：トラヒック制御装置

本手法により、トラヒック制御装置は内部ネットワークからは通常の P2P ノードに見えるが、外部ネットワークからは接続性の悪い P2P ノードと判断される。このため、外部ネットワーク上の P2P ノードは制御装置からのファイルのダウンロードを避けるようになる。さらに P2P ノードの自律分散的な動作により、P2P ネットワークの構造が実ネットワークの形状に適応した形に変化する事も期待できる。

4. おわりに

本稿では、TCP フロー解析に基づき P2P トラヒックを制御し、ISP 間の P2P トラヒックを軽減する手法を提案した。具体的には、P2P アプリケーションが構築する論理的ネットワーク (P2P ネットワーク) 上のトラヒックを収集し、P2P フローの分類を行なった。この P2P トラヒック特性を利用し、P2P ネットワーク上にファイルキャッシュを実現し、ペイロードやセッションを監視せず ISP 間のトラヒックの軽減する。最後に日頃ご指導頂く KDDI 研究所浅見徹所長に感謝する。

参考文献

- [1] 亀井他, “P2P ファイル共有の実態と課題～トラヒック測定・設計・制御・管理手法の確立に向けて～,” 信学技法 CQ2003-40, Sep. 2003.
- [2] P-Cube Inc., “Approaches To Controlling Peer-to-Peer Traffic,” Technical White Paper, <http://www.p-cube.com/>.