マルチメディア通信と分散処理 92－13
（1999．2．26）

インターネットのトラフィック計測とその分析

安田 豊

神戸大学 経済経営研究所

ネットワークアプリケーションが全体として効率良く機能するためには、実際のインターネットのトラフィックを計測し、分析することが不可欠である。本稿では多様な分析を可能にするトラフィックデータを長期に渡って収集し蓄積することができるトラフィック計測システムを提案する。さらにこのシステムを用いて実際に複数のサイトにおいて測定したデータをもとにトラフィックの集中に関する分析を行ない、その有用性を示す。

Monitoring and Analyzing of the Internet Traffic

Yutaka Yasuda

Research Institute for Economics & Business Administration of Kobe University

The monitoring and analyzing of the Internet traffic is indispensable to optimize the network application behavior. This paper shows a traffic monitoring system that can collect and archive the traffic data in long time period for various analysis. And the advantage of it is shown by the analyzing about the traffic concentration which is based on the data that was captured on several sites.

1 はじめに

インターネットの利用が普及するにつれて、ネットワークアプリケーションは単体で正しく動作するだけでなく、全体として機能することが重要な課題となってきている。すなわち各アプリケーション単体の動作を検証するのと同じように、全体として効率良く動作するための検証が求められている。これはすなわちアプリケーションが全体として無駄なトラフィックを要求せず、効率良くネットワークを利用することを意味している。

この利用最適化はインターネットにおける重要な課題の一つであるが、トラフィックに注目した最適化を検討するには、現実のインターネットのトラフィックの特性をまず明らかにする必要がある。それにはインターネットを実際に流れているトラフィックを測定、蓄積し、分析することが重要である。しかし今のところ、そのような目的で収集し公開されたトラフィックデータは少なく、必要な分析を行なうための情報を得ることは容易ではない。

本稿では、必要な詳細度で適切なトラフィック情報を収集するシステムを開発したのでまずそれを報告する。そしてこれを用いて大学、商用プロバイダにおける実際のインターネットトラフィックを計測、収集した。後半ではこうした計測データをもとに、主要アプリケーションのトラフィックの集中傾向に関する分析について報告する。

2 トラフィック計測システムの開発

トラフィック計測システムは一般に高価であり、あまり普及していない。後の多様な分析を可能にするためには、パケットのヘッダ情報を蓄積する必要があるが、簡易なパケットモニタを用いて単純に全トラフィックのパケットヘッダを収集して

いたのでは、短期間のうちに蓄積することが困難な規模のデータ量になってしまう。仮にデータを蓄積できたとしても、後に分析に利用する際のハンドリングは非常に困難なものになろう。

すなわち、ネットワークを流れる全パケットをチェックし、必要な情報だけを適切な形で効率良く蓄積するシステムが必要である。これがトラフィック計測システムを開発した理由である。

2.1 配置

各サイトにおけるインターネットのトラフィックとは、具体的には各サイトの LAN とインターネットを接続しているルータを通過するトラフィックを意味する。この計測を可能にする方法はさまざまであるが、今回開発したトラフィック計測システムは多くのサイトにおいてインターネット接続ルータが Ethernet インタフェイスで LAN 接続されていることに注目し、その Ethernet セグメントにトラフィック計測システムを接続することとした。すなわち接続された Ethernet セグメントを流れるパケットを傍受し、送り元及び宛先 IP アドレスからルータを越えると考えられるパケットを選別するのである。

2.2 構成

開発したトラフィック計測システムの実体は、Pentium II 266MHz CPU / 128MB RAM / 4GB HD の PC/AT である。ネットワークインタフェイスには 10Mbps/100Mbps 両用のものを利用しており、10Mbps と 100Mbps どちらのインタフェイスでルータ周辺を構成しているサイトでも計測可能となっている。OS には Linux を用いた。

計測プログラムは libcap0.4a-5, tcpdump3.4 [1] をベースに開発した。具体的には tcpdump からトラフィック計測に不要な機能を取り除き、必要なヘッダ情報だけを収集して出力するように作り変えている。このヘッダ情報収集プログラムを pdump と呼ぶ。pdump が出力する情報は 1 パケットあたり 20 Bytes に過ぎないが、蓄積に際しては更に簡約化を行なうプログラムを開発して、必要な統計情報だけを残すことも可能にした。この結果、1.5Mbps のインターネット接続環境で、余裕を持って長期間トラフィック情報を収集できるシステムを構築することができた。

以下に、各プログラムの働きについて説明する。

2.3 採取する情報

今回のトラフィック計測では、パケット長、送り元 IP アドレス、宛先 IP アドレス、プロトコル種別、Time To Live、送り元ポート番号、宛先ポート番号を収集することとした。ICMP などでは、ポート番号の代わりに Type code などが入る。更にパケット通過時刻も必要であるが、これはパケット自身には含まれないため、トラフィック計測システムが加えることになる。

記録されるのはもっぱらパケットのヘッダ情報であり、ユーザがやりとりしているデータ内容については全く参照しない。値は全てネットワークバイトオーダーで格納される。

内容	Bytes	備考
時刻	4	1970 年 1 月 1 日から数えた秒数 (GMT)
パケット長	2	ヘッダを含めた IP パケットの全バイト数
送り元 IP Addr.	4	
宛先 IP Addr.	4	
Type	1	TCP/UDP etc.
TTL	1	
送り元 port No.	2	
宛先 port No.	2	

図 1: pdump 記録情報

IP パケットが一つ通過するたびに、pdump プログラムはこの 20 バイトを記録していく。実際に 1.5Mbps 回線の計測を行なってみると、一日の合計転送量が 4GB から 6GB であった場合、記録されるヘッダ情報は 1GB 程度、1 時間あたり 20MB から 40MB 程度となる。

2.4 情報の集約

例えば特定のサイトの単位時間ごとのアプリケーション別転送バイト量を調べるなど、パケット単位で詳細に追跡する必要がない分析のために、情報を更に簡約化して一日あたりの記録データ量を小さくすることを試みた。

この目的のために undump, summary 各プログラムを開発した。undump プログラムは図 1 に示したヘッダ情報を以下の情報で分類し、アクセス先サイトとサービスごとに単位時間あたりのパケット数とバイト数の合計だけを可視化して出力する。これによって、例えば一つの telnet セッションによってながれた数百以上のパケットの情報が、せいぜい数行、数百バイトに集計される。

図 2 に undump による集計結果の例[1]と、各出力項目の内容を示す。

```
I 204.137.47.14     2     237 : UDP domain peer
O 204.70.214.123   20    1160 : ICMP echo-req clnt
I 206.137.47.2     18    4188 : TCP smtp clnt
I 201.23.168.5    119    4807 : TCP telnet clnt
O 132.87.38.25    402   35292 : TCP www clnt
I 203.253.46.10   150   56779 : TCP www serv
```

内容	備考
パケット方向	Incoming / Outgoing
宛先	サイト内のホストと通信している相手の IP アドレス
パケット数	
バイト数	単位は Bytes
Type	TCP/UDP etc.
port	サービスの種類を示す
サービス方向	サービスの方向を示す

図 2: undump 記録情報

時間情報はファイルの名前として記録する。パケットの方向は、取得したパケットの IP アドレスの送り元、宛先情報から判断する。サービスの方向（自ネットワークのホストが、サーバ側かクライアント側か）は、パケットの方向とポート情報から割りだしている。

[1]例示で用いた IP アドレスは架空のものである。

```
I 203.253.46.10   150   56779 : TCP www serv
```

例えば上の例は、計測サイト側から見て、サイト内ホストがクライアントとなって、サイト外ホストである 203.253.46.10 に WWW のアクセスをした結果、サイトに入ってきたパケットが、単位時間あたり 150 パケット、そのパケットの合計データ量が 56,779 バイトであることを表している。

この集計を行なう単位時間を 10 分間とした結果、前節に示した pdump が出力した 24 時間で 4GB から 6GB になる情報を、4MB から 5MB 程度と 1/1000 程度に集約することが出来た。もちろん通信先が増えるなり、単位時間を短く刻むなりすれば記録するデータ量は増える。

summary プログラムは、これらの集計情報を、更に指定の項目によって集約する。例えば undump を用いて 10 分単位で採取し、集計した結果ファイルが 6 つあった場合に、これを集めて 1 時間単位の集計結果を求めることができる。また特定の項目に注目し、それ以外の情報の相違を無視して集計しなおすこともできる。例えば TCP/UDP/ICMP のプロトコル情報に注目して集計し直すと、先の例は以下のようになる。

```
- -          689  101066 : TCP - -
- -           20    1160 : ICMP - -
- -            2     237 : UDP - -
```

summary プログラムはこのように注目する項目を自由に設定でき、分析に必要な情報を必要な時間的詳細度で集計することが可能である。これによって更に必要な情報だけを蓄積し、取り扱いを容易にすることができる。

undump+summary による集計作業は pdump と同時並行で一台のマシンに行なわせているが、それでもパケットをとりこぼすことなく、安定して処理し続けられる性能を維持している。

3 トラフィックの分析

このトラフィック計測システムを用いて実際に行なった計測と、それに基づいて行なった分析について示す。

3.1 計測の地点と期間

現在までに連続的なトラフィック計測を四箇所において行った。期間はいずれも一カ月間から二カ月間であり、本稿では計測を行なった順にそれぞれ Site A, B, C, D と呼ぶ。

Site A, C は、それぞれインターネットの leaf に位置する学生数一万人以上の大学である。バックボーンへの接続速度はともに 1.5Mbps である。

Site B は、商用の ISP (Internet Service Provider) である。バックボーンへの接続速度は 1.5Mbps である。主たるサービスはレンタルサーバ、ホスティングサービスなどであり、ダイアルアップ接続サービスは提供していない。

Site D も商用の ISP であるが、こちらはレンタルサーバ、ホスティングサービスに加えて数百回線に及ぶダイアルアップ接続サービスも提供している。バックボーンへの接続速度は 4.5Mbps である。

3.2 トラフィックの集中

上記 4 サイトで計測したデータをもとに、ネットワークアプリケーションのトラフィックの集中について分析を試みた。

3.2.1 分析する上での問題

トラフィックデータをサイトごとに集計する場合、単純に IP アドレスごとに集計するだけでは済まない。例えば www.yahoo.co.jp[2]は DNS ラウンドロビンによって 5 つの IP アドレス、それも同一場所にあると思われるアドレスに振り分けられている[3]。このような場合には IP アドレスは別でも同一 WWW サイトに対するアクセスと認識する必要がある[4]。実際にこれらを集計してはじめて、Yahoo Japan サイトへのアクセスが、多くの時間帯で上位 10 位以内、ピークタイムでは安定して 5 位以内に入っている事実がわかる。そこで、次の分析では収集した IP アドレスからホスト名の逆引きを行ない、同一サイトと思われるトラフィックは集計した。逆引き出来ないサイトに関しては可能な限り手作業で追跡、確認している。

[2]著名なサーチエンジンサイト、yahoo.com の日本版。

[3]1999 年 1 月現在。

[4]勿論分析の目的次第では別サイトへのアクセスと考えるべきケースもある。

3.2.2 WWW トラフィックの集中

まず、WWW が発生させるトラフィック集中を以下に示す。図 3 に Site C における、ある一週間の平均の一日分の、各時間ごとの転送データ量のうち、トラフィック上位のサーバがどれだけを占めているかを示す。該当一時間当たりの WWW サーバのサイト数を m として、その 0.1% である上位 $m/1000$ サイト、$m/100$ サイト、$m/10$ サイト、それ以下のサイトの、転送データ量合計を積み上げて縦軸に取っている。ピークタイムをグラフの中央に寄せるために、時間を示す横軸は午前 8 時から始めていることに注意されたい。

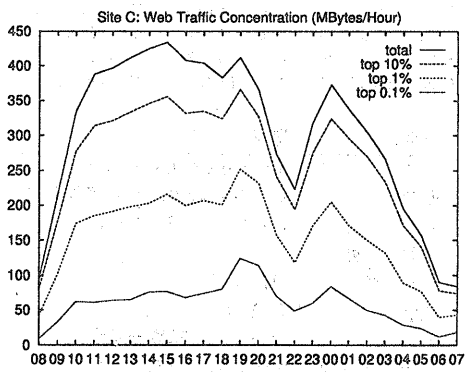

図 3: WWW における集中 (Site C)

時間帯に関係なく上位 0.1% のサイトが 20-25% 程度、1% のサイトが 50% 程度のトラフィックを占めていることがわかる。上位 10% のサイトまで含めると 80-90% 程度のトラフィックである。サイト数にして 90% を占める、残りの WWW サーバは、転送量にして 10-20% 程度しかトラフィックを出していない。

実数で見ると、Site C において一時間にアクセスした WWW サーバの数は、ピークで約 8200 サ

イト、少ない時間帯で約 1800 である。すなわち上位 0.1% とは、多いときでもせいぜい 8 サイトに過ぎない。少ないときで 1、2 サイトである。常にこれら非常に少数の特定サーバに、桁外れのトラフィックが集中していることがわかる。この傾向は Site A, D でもほぼ同様であった[5]。

3.3 アプリケーションごとの集中傾向

前節で示した指数的な集中は WWW だけではない。代表的なアプリケーションである SMTP, DNS にも同じ傾向が見られた。図 4 に、Site C, D における各アプリケーションごとの集中傾向を示す。サイトの集約は前節ほど厳密ではなく、IP アドレスを 24bit netmask 位置で集約することで行なっている。グラフはある一週間にアクセスがあったサイトのうち、最もアクセスの多かったサイトを左から順に並べ、縦軸に転送バイト量を示したものである。軸は共に対数軸である。WWW についてはサイト外のサーバへのアクセスだけを対象にしているが、SMTP と DNS は送受信両方を対象とする。

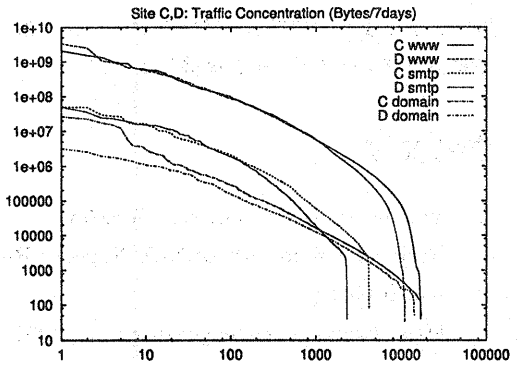

図 4: アプリケーションごとの集中傾向 (Site C,D)

一見して三つのアプリケーションがほとんど同じ集中傾向を示していることがわかる。WWW リクエストの回数は Zipf の法則に従うという報告 [3] があり、図 4 における WWW トラフィックはそれをほぼなぞっているが、SMTP と DNS についてもほとんど同じカーブが現れている。

なお、バイト転送量は DNS を基準にして SMTP が一桁、WWW が三桁ほど多く、相手先サイト数は DNS と WWW がほぼ同数、SMTP がその 20-25% 程度であり、これも各サイトで同じ傾向を示す。ただし Site C では第 4 位ごろまで WWW, DNS ともに突出する傾向を見せているが、他のサイトではこの傾向は現れていない。

グラフにとりあげた Site C, D はともにクライアントとなる利用者が一万人以上存在するサイトであるが、目立つ共通点はその程度である。C は大学であるのに対して D は商用 ISP であり、C は日中学内端末からのアクセスが主であるのに対して D は夜間のダイアルアップ接続ユーザが主であることなど相違点は多い。それにもかかわらずアプリケーションの利用率、アクセス傾向が似ていることは興味深い。

続いて各アプリケーションの特性を明確にするために、Site D を用いて順位と転送バイト量の最大値を揃えるように標準化したグラフを図 5 に示す。

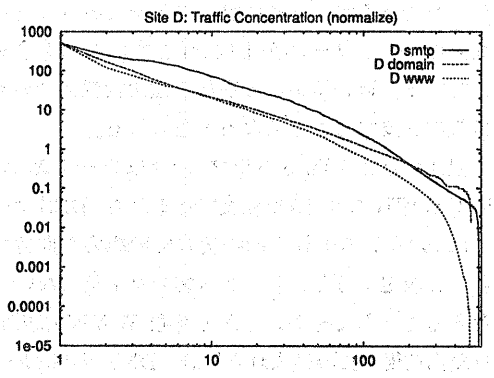

図 5: 標準化した集中傾向 (Site D)

これにより各アプリケーションのトラフィック特性の相似がより明確になった。特に DNS と WWW のグラフ左側における相似は顕著である。右側で

[5] Site B には WWW アクセスを行なうクライアントがほぼ存在しないので比較には適切でない。

はWWWトラフィックが他のサービスに比べて早期に下降しはじめる。全体で注目すべきは各カーブの下降度そのものであり、これはすなわち集中の度合いを示す。グラフにおける下降の角度が緩やかであるほど上位サーバに対する集中の度合いは弱く、その意味でDNSとWWWはほぼ同じ程度の集中度を起こしていることになる。SMTPはそれに比べて緩やかであり、主要なサーバがより分散していることを示している。

WWWはインターネットにおける主要なトラフィックを占めているが、現在のところ有効に機能するトラフィック広域分散化の仕組みを持たない。それに対してはじめから分散化のための仕組みを持っているはずのDNSが、WWWと同程度の集中を起こしてしまっているのである。これはインターネットにおいてDNSがその分散化機構を有効に機能させられないような運用状況になっている可能性を示唆する。

現在のところgTLDではcom, orgなど第一レベル、jpドメインではac.jp, co.jpなど第二レベルの、細分化される直前までが共通のDNSサーバ群で処理されている。収集したデータにもそれが反映されており、DNSトラフィックのうち上位5サーバまでは、ns1.nic.ad.jpなどのjpドメインサーバであるが、それに続いてb.root-servers.netなどのルートサーバが上位20位内に8つも含まれている。近い将来この現在の運用状況について再検討を要することになると思われる。

現在のところDNSトラフィックはデータ量においてWWWの1/1000程度であるため、DNSサーバにWWWのそれと同程度の処理能力を期待できると仮定すると、サービス能力は不足しないと考えることもできる。しかし今後WWWに広域分散化技術が組み込まれた場合、DNSがインターネット中最も集中を発生させるアプリケーションとなる可能性もある。

これらのことについては、更に多くのサイトにおけるサンプルを得て分析を続けたいと考えている。WWW同様に特に広域分散化の工夫がないSMTPが、WWWやDNSよりも分散する傾向を示している理由についても未検討であり今後の課題である。

4 まとめ

インターネットが将来重要なインフラとなるために必要な、アプリケーションのネットワーク利用最適化を検討するために、まずインターネットのトラフィックを計測するシステムを開発した。これによって数カ月にわたる長期のトラフィック計測が安価なPCによって可能であることが確認できた。

また、これを用いて何箇所かのサイトのトラフィックを計測した結果、主要なアプリケーションがいずれも似た特定サーバへの集中傾向を示すことがわかった。特にアクセスの広域分散化のための機構をもつDNSが、それをもたないWWWと非常に相似的な傾向を持つことが明らかになった。

今後、更にトラフィック計測システムを改良しながら多くのサイトでの継続的な計測を行ない、アプリケーションのネットワーク利用最適化の可能性などについての検討を行なう予定である。計測システム及び計測データの公開などについても検討し、より多くの研究者やアプリケーション開発者にトラフィックデータを提供したい。

参考文献

[1] Van Jacobson 他, Lawrence Berkeley National Laboratory LBNL's Network Research Group, http://www-nrg.ee.lbl.gov/nrg.html, 1998

[2] 串田高幸, "インターネットのトラフィックを使用した課金体系", 情報処理学会研究報告 Vol.98-DPS-88, 1998

[3] 西川記史, 細川貴史, 辻洋, 森靖英, 吉田健一, "WWWトラフィック分析と分散キャッシュ", 情報処理学会研究報告 Vol.97-DSM-5, pp.7-12, 1997