

TCP/IP ネットワークにおけるトラフィックの特徴

串田 高幸

日本アイ・ビー・エム株式会社
東京基礎研究所

本研究では、インターネットの状況を正確に把握するためにインターネットにおけるトラフィックの収集方式を確立することを目的としている。本稿では、まずトラフィック収集と解析について、その成り立ち及び関連した研究について述べる。そして、トラフィックの収集と解析について、目的、装置の種類、トラフィック流れの定義、解析の分類及びサブシステムの機能について説明してゆく。そして実際にシステムを使ってインターネットのデータを解析した結果について報告する。データの解析の結果、ネットワークのトラフィックは、全データ量のうち、UDP が2%程度であって TCP は97%程度であった。また TCP のうち、FTP が3%から18%ぐらいであり、WWW は58%ぐらいであった。一方、UDP は、DNS が99%を占めていることがわかった。

はじめに

最近、一般へのインターネットの利用が急激に伸びている。インターネットは、当初、主として研究機関や大学で利用されるためのネットワークとして設立された。そのため、研究教育機関の間の連絡や情報共有のための通信手段として広く利用されてきた。その後、インターネットの有用性が認識され、利用者が研究教育以外の一般の人に広がってきた。そして研究教育の機関以外の多くの組織がインターネットに接続されるようになってくると利用形態も多様になり、ユーザーの要求も多様になってきた。そのため、各種の新しいアプリケーションがインターネットで開発されて使用されるようになってきている。つまり、インターネットにおいて、ユーザーの種類が変化すると、それにつれてネットワークで利用されるアプリケーションも変化してきている。この変化のうち最も顕著なのは、従来から使用されているファイル転送サービスの FTP や電子メールサービスの SMTP が、WWW や実時間オーディオ転送あるいは実時間ビデオ転送に変わったことである。しかし、WWW や実時間転送アプリケーションのような新しいアプリケーションでは、高トラフィックあるいは一定スループットをアプリケーション側から転送することをネットワーク側に要求している。

一般に「インターネット」という言葉は、TCP/IP プロトコルを使用して相互接続されたパケット交換ネットワークの一群の意味で使用されている。インターネットで

は、ネットワークの中をパケットあるいはデータグラムと呼ばれるデータの断片がルーターによって転送されている。ネットワークの中のルーターは、以前よりルーター内に持っている経路情報のアドレス表と転送されてきたパケットのヘッダーに記録されている目的アドレスとを比べて、適切な次のルーターにパケットを転送することを行なっている。この転送が、ネットワーク内の始点から途中のすべてのルーター、そして終点まで正しく処理が行なわれることによって、最終的に目的ホストにパケットが到達することになる。

このようにインターネットでは、パケットが転送を行なうための最小単位になっている。インターネットにおいて、ネットワーク上を流れているパケットを収集して、パケットヘッダーを解析していくことにより、ネットワークの状態を正確に把握することができる。また、ネットワーク内のパケットの流れを解析した結果をもとにして、将来のトラフィック予測したり、現在の混雑の状況を調査したり、あるいはトラブルを未然に防いだりすることができる。さらにインターネットのトラフィックの測定を行ない、その解析結果によって将来のネットワークへの拡張計画に対する基本資料として利用することもできる。このようにネットワーク管理の観点からみていくと、上に述べたトラフィック解析をもとにしたアプローチは、ネットワークにおける維持管理及び計画に対して今後、重要な要素になってゆく。また管理側だけではなく、ネットワークを利用しているエンドユーザーにとってもトラフィックの混雑状況の予測が事前に揭示されれば、その利用を前もって避けたり、あるいは

利用するホストや時間を変更するという具体的な方策をたてることができる。そのため、エンドユーザーへのトラフィックの表示は、今後、インターネットにおいて大切なアプリケーションの一つとなってゆくであろう。また現在、インターネットのトラフィックの収集解析に関する理論、そしてそれをもとにしたツールやデータ収集及び解析方式が、まだきちんと確立されていない。そのため、そのような種類のツールが一般に広く利用されるまでに至っていない。このようなことからトラフィックの収集及び解析に関する研究開発は、ネットワーク管理の一つの機能として今後、ますます必要不可欠な分野になると考えられる。

一方、トラフィック解析には、ネットワーク全体のトラフィックを解析する方式以外に特定のアプリケーションに限定したトラフィックを解析する方式がある。例えば、WWW についてのアクセス状況を解析する方式である。アプリケーションを WWW に限定した理由は、インターネットのアプリケーションのうち特に WWW の利用が急激に伸びており、その利用状況を的確に把握する要求が出てきているためである。WWW サーバーでは、そのアクセス頻度を知るためにサーバーの中のプログラムにおいてホームページの参照数をアクセスログとして記録する機能を持っている。このアクセスログを収集し解析を行ない、その結果をヒット数あるいは参照回数として求めることで WWW が、現在どの程度利用されたかを調査することができる。WWW のアクセスログの内容は、時間、相手のホスト名、要求された URL、転送量等である。しかし、この方式では、単に一つのサーバーにおいて、どのホームページが利用されたかということだけしかわからない。他の WWW サーバーとの比較は、他のサーバーで取得したデータと比較することが必要となってくる。この問題を解決するためにテレビの視聴率と同様にサンプルとしてアクセスするユーザーを事前に登録しておき、そこに専用の収集用ソフトウェアを設置して、アクセス数を記録しておく。そこで集められたサンプルのデータにより母集団を推定する方式が使用される。しかし、ネットワーク全体で見た場合に分散している個別のサーバーで収集したアクセス状況をまとめて解析する方式よりもトラフィックが集中しているバックボーンノードにおいて、ネットワークのトラフィックからアクセス状況を解析した方式の方が、より安定して正確な解析を行なうことができる。

我々の以前の研究では、インターネットのネットワークの状況を正確に把握するためにインターネットのトラフィックの全パケットの収集システムを構築することを行なった。そして、そのシステムを利用して実際のインターネットのデータの収集を行なったことを報告した

[12]。そして、収集したデータからトラフィックの解析を行なったことについても報告を行なっている [13]。

この方式では、全パケットを収集するために統計的な手法を使ってサンプルから母集団を推測をする必要がない。そのため、正確なトラフィックの結果を出すことができる。また全パケットを収集しているためにパケットのサンプリング方法を変更することにより、最適なサンプリングで収集するパケットの数を減少させることができる。例えば、収集するパケットを 1 時間に一度、10 分間だけ収集して、単純な確率分布により 1 時間の全トラフィックを推定する方法をとることもできる。また、個別のパケットをすべて収集しているために、例えば、セッションごとのプロファイルの測定、パケット間ギャップの分布あるいはパケット長の分布などのデータも取得することができる [1]。

関連する研究

米国のインターネットにおいてネットワークの一般の利用に主導的な役割を果たした NSFNET では、全米に展開した T1 及び T3 のバックボーンの各拠点においてトラフィックの収集が行なわれていた。NSFNET では、トラフィック収集の目的のためにバックボーンの各サイトにある NSS(Nodal Switching Subsystem) によってネットワークのトラフィックデータを取得するために専用機能が組み込まれていた。その結果、NSFNET プロジェクトでは、バックボーンのトラフィックにおける長期的な傾向について詳細な報告を行なうことができた [2]。また NSFNET バックボーンにおけるトラフィックの詳細な特徴のデータについても報告された [3]。

トラフィックの特徴を解析して理解するためにデータのサンプリング方式が重要になる。トラフィックの特徴を収集するためのサンプリング方式には、1) 時間をトリガーとする方式と 2) パケットをトリガーとする方式がある。しかし、両者の解析結果が必ずしも同じ結果にならないことが報告されている [4]。これは、データのサンプリングを行なうとき、サンプリングの方式を注意深く選ばなければならないことを示唆している。

トラフィックの解析においては、対象となるトラフィックへどのような数学モデルを適用するかが重要となる。向う 1 年の NSFNET バックボーントラフィックを予想するために時間モデルとして、ARIMA(AutoRegressive Integrated Moving Average) が、よく一致することが報告されている [6]。またこのモデルを使うと、2-3 年先のトラフィックの予想にもだいたい合うようことが報告されている。

一般にパケット交換ネットワークでは、受信側においてネットワークからのパケットの到着時間の確率分布は、ポアソン分布になることが以前より知られている。

しかし、Paxon らは、リモートログインやファイル転送のようなユーザーが起動する TCP セッションの場合には、その到着時刻の分布が、ポアソン分布に、よく一致することがわかっている。しかし、それ以外のトラフィックは、ポアソン分布とは全く異なったモデルになることを報告した [7]。

TCP/IP プロトコルを使うネットワークは、エリアで分割すると LAN(Local Area Network) と WAN(Wide Area Network) に分かれる。この LAN と WAN では、トラフィックモデルが、まったく全く異なることが報告されている [8]。LAN におけるトラフィックモデルは、統計によって適用するモデルがない self-similar 形式になることが報告されている。この結果は、3 年間以上の Ethernet のデータの収集により収集された LAN のデータを統計的に解析した結果によって裏付けがなされている。

実際のインターネットにおける実験として End-to-end でパケット転送の実験を行なって、その結果を解析してインターネットの特徴を報告している [5]。この実験の解析の結果、End-to-end で見た場合にインターネットでは、約 2 パーセントから約 10 パーセントのパケットを損失としていることがわかった。また周回遅延の変動は、ネットワーク中を横切っているトラフィックにより影響を受けることが原因だけでは、説明がつかないこともわかった。またインターネットでは、パケットが転送されているときに、数多くのパケットの順番の入れ替わりやパケットの重複があることもわかった。さらにこれらの現象は、トラフィックのロードが軽い場合でも起こっていることがわかった。もしパケットの損失がパケットバッファでのオーバーフローにより引き起こされているならば、結果として周回時間の増加もあるはずである。しかし、これはケースバイケースであると報告されている。そのため、パケットのバッファのオーバーフロー以外の別の理由もあることが結論づけられている。また、個別の損失の原因が、ランダムビットエラーであるとは結論づけられなかった。この個別に起こる損失は、サーバーとクライアントの間の同期の問題であると推論された。例えば、クライアントから送られてきてサーバーで受信するパケット間の時間が短いと最初のパケットを取り出した後に次のパケットを落としてしまうことで説明できると報告している。またサーバーからの応答に一秒以上の遅延があることが認められたが、これはネットワーク内でのトラフィックの遅延という理由よりも、むしろコンピューター内部の入力による遅延であると理由づけられる。またサーバーが入力処理をしたときに、特定の時間、パケットをキューしてしまい処理していないことがある。この問題についてもその報告

では指摘している。

また、特定のアプリケーションとしてインターネット上のホスト名と IP アドレスの分散名前データベースである DNS(Domain Name System) のトラフィックの解析を行なった結果について報告された [9]。DNS のトラフィックを実際のインターネットの DNS において 24 時間のトラフィックを収集して、その解析を行なったことについて報告している。そして、その報告では、DNS の設計上及び実装上の問題点を示した。もし DNS において、効果的なキャッシングとタイムアウトの再処理を行なうことができれば、広域ネットワークにおける DNS のトラフィックの転送量を効果的に減少させることができることが報告された。このことは、トラフィックの観点から見ると、広域ネットワークのアプリケーション間におけるキャッシングとタイムアウトの技術は、トラフィック量の効率のよい転送にとって非常に大切であることがわかる。

ネットワークトラフィック用のツールに関して、プロトコルの実装のトラブルを単純化するためにネットワーク上のデータをチェックすることを主な目的としたネットワーク測定ツールが報告されている [10]。このツールは、インターネットのパケットをモニターするためにプロトコルの流れについて、その表示をテキストタイプにして視覚化している。ネットワーク管理の観点からトラフィックの解析は、信頼性のあるトラフィックの収集と統計的な解釈にもとづいて行なわれる。以前のツールではパケットのトレースは、パケットヘッダーをそのまま表示することだけに限られていた。このツールでは、単にトレース結果を表示するだけでなく、プログラムによって効果的にディスプレイ上に、別な観点からの解析結果を表現するための機能を入れた。

トラフィックの収集と解析

本章では、トラフィックの収集と解析について 1) 収集及び解析の目的、2) トラフィック測定装置の種類、3) トラフィックの解析の分類及び 4) トラフィックの収集の手順について説明行なう。

収集及び解析の目的

トラフィックを収集し解析することに対する目的を以下のように分類した。

- 現在のトラフィックの状況を解析行なうこと
ネットワークのトラフィックを測定した時点におけるトラフィックの状況を調査することが目的となる。この解析によって、ネットワークがどのようになっているかがわかる。
- 長期間の収集によるネットワークのトラフィックの連続的な変動を調査すること
過去から長期間に渡り連続的にトラフィックの変

動を収集して、その変動を記録してゆく。この記録を解析することにより長期の予想が可能となる。

- 将来のネットワークの新設や変更に対する基礎データを集めること

ネットワークの計画的な新設や変更に対して、ネットワークでの使用状況の基礎データを集める。そのデータをもとにして、新設や変更の計画を立案してゆく。

- 長期の測定により定常値を求めて、そこからトラブル時の異常値を検出すること
長期間測定をすることによって、日常的变化を考慮した定常値を導きだして、そこからの有意の差によって、トラブル時の異常値を検出することができる。この方式は、ネットワーク管理に対して有効である。
- エンドユーザーに対するトラフィック状況の提示
エンドユーザーに対して、混雑度や到達時間についての表示について、トラフィックを収集することにより行なう。エンドユーザーは、情報を与えられることによって混雑の事前の回避が可能となる。

トラフィック測定装置の種類

またトラフィックの収集と解析は、その利用用途や測定時間の長さあるいは、解析の粒度によってネットワークモニターとネットワークアナライザーの2種類のツールに分類することができる。

- ネットワークモニター (マクロの視点)
長期に渡って連続的に日常のトラフィックデータを収集する方式である。この方式では、統計情報としてのネットワークにおけるデータの収集を行なうことができる。最終的には、それぞれの項目を加算したデータを使用してトラフィックの解析を行なう方式である。
- ネットワークアナライザー (ミクロの視点)
プロトコルの解析、イベントトリガーによる測定及び問題点の発見など、一時的にかつ局所的に使用するための方式である。また、この方式では新しいプロトコルの開発時のプロトコルテスターとして利用することができる。ネットワークアナライザーでは、特定のデータを集めて、そのデータを解析的な表示として、問題となっている箇所の解決を行なう方式である。

トラフィックの流れの定義

またトラフィックの流れの定義は、次のように分類される。

- 流れの方向性

図1が、流れの方向性である。トラフィックの流れが、双方向か片方向であるかに分類されることが

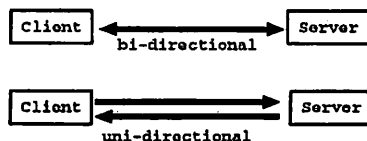


図 1: 流れの方向性

できる。一般に TCP は、双方向のストリーム型のパスを作るプロトコルである。例えば、TCP のセッションが確立された後の二つのホストをそれぞれ Client と Server とする。通常、アプリケーションでは、Client から Server への片方向にデータパケットが転送される。しかし、そのとき逆方向の Server から Client へも ACK だけが入った制御パケットが転送される。その場合、トラフィックの流れが片方向であると言うことができる。また TCP において、Client から Server へデータが転送されていると ACK とともに同時に Server から Client へデータが流れている場合に、その状況をトラフィックの流れが双方向であると言うことができる。通常、アプリケーション間のプロトコルは、ある時点を取ってみると片方向のトラフィックである。そのため、簡易に調べる場合には、方向性に関して片方向を調べればよいことになる。

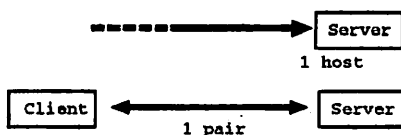


図 2: 1つの終端点か2つの終端点

- 1つの終端点か2つの終端点

図2が、1つの終端点か2つの終端点である。通常、トラフィックは、始点から終点に流れてゆく。そのとき、始点あるいは終点だけに注目してトラフィックを測定することを「1つの終端点の測定」と定義する。また始点と終点の一对に注目してトラフィックを測定することを「2つの終端点の測定」として定義する。このように終端点をどのように見るかでトラフィックの流れの定義が変わる。インターネットのトラフィックの場合、IP アドレスや IP アドレスの集合で表わされているネットワーク番号、また UDP や TCP の各トランスポート層のポートがパケットヘッダーに記録されている。これらの値は、必ずソース側と目的側の一对になって入っている。

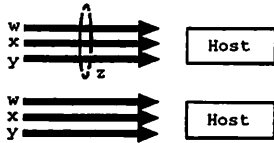


図 3: トラフィックの終端点での粒度

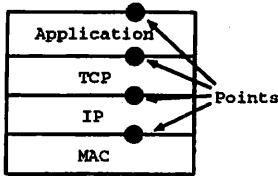


図 4: プロトコルの階層

例えば、ネットワーク番号 1 のホスト A のポート X からネットワーク番号 2 のホスト B のポート Y へトラフィックが流れている例を考える。その場合、1つの終端点では、ホストの場合、A と B のそれぞれ、ネットワーク番号の場合、1 と 2 のそれぞれ、ポートの場合、X と Y に注目することになる。また、2つの終端点では、ネットワーク番号 1 からネットワーク番号 2 に流れるトラフィックあるいは、ホスト A からホスト B へ流れるトラフィックに注目することになる。

● トラフィックの終端点での粒度

図 3がトラフィックの終端点での粒度である。この方式では、言い換えるとトラフィックの束ね方になる。つまり、終端点を何にするか定義して、注目するトラフィックの粒度を決めてゆくことである。粒度が大きいか小さいかによって注目しているトラフィックの意味が変わってくる。

例えば、注目しているトラフィックが、ホストごとであるのか、アプリケーションごとであるのか、あるいはネットワークごとであるのか、組織ごとであるのか、ネットワークプロバイダーごとであるのか、地域ごとであるのか、国ごとであるのか、ということで分類することをいっている。

● プロトコルの階層

ネットワークの流れをプロトコルの階層により解析することができる。インターネットには、ネットワーク層として IP のプロトコルがあり、またトランスポート層として TCP/UDP のプロトコルがある。またアプリケーション層として、各種のアプリケーションがある。例えば、解析する場合に、ある時点ではトランスポート層の接続開始と接続終了の流れに注目するが、また同じ流れを

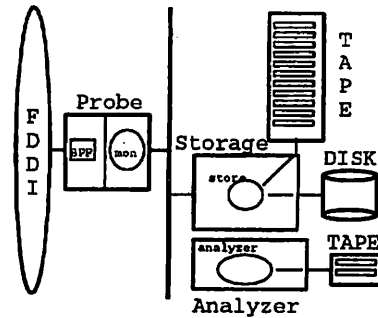


図 5: 収集解析システム

アプリケーション層の流れに注目することもできる。また、単一のトラフィックの流れであっても複数の TCP 接続が集まっている場合もあって、さらに UDP パケットや TCP 以外のパケットが、TCP パケットの間に挿入されることもある。

トラフィックの解析の手順

インターネットにおいて収集するトラフィックの収集量およびその種類については、プロトコルの階層ごとに次の項目に分類することができる。

● 全トラフィック

測定しようとしているネットワークに流れている全トラフィックのデータの転送量を取得する。

● ネットワークごとのトラフィック

ソース IP アドレスと目的 IP アドレスのホストごとに、さらにネットマスクを含んだネットワーク番号のホストごとでネットワーク上の転送量のトラフィックを取得する。

● 各プロトコルごとのトラフィック

インターネット層あるいはトランスポート層ごとのトラフィックを取得する。例えば、インターネットであれば、UDP と TCP プロトコルの転送量、それ以外のプロトコルの転送量についてのトラフィックの取得する。

● アプリケーションごとのトラフィック

アプリケーション層においてトラフィックを取得して、アプリケーションごとの転送量を測定する。インターネットでは、アプリケーションとして、WWW、FTP、SMTP、NNTP 及び DNS のような個別のアプリケーションごとの転送量を取得してゆく。

それぞれのクラスに分けることができる。これらのクラスのそれぞれには、パケット数とバイト数の 2つの単位の転送量を測定することができる。この分類に加え

てトラフィックを収集した時間間隔が入っているので、さらに時間に対するクラスも持つことができる。

トラフィックの収集装置

パケット交換ネットワークにおけるトラフィックの収集と解析に対する手続きをまとめると次のような項目に分類できる [12]。

1. 全データの収集 (Probe)

ネットワークに流れている全パケットをプロトコルや種類によらずに収集するための機能のこと。

2. 規則による取り出し (Filter)

全パケットを事前に定義した規則にもとづいてデータの取り出しを行なうことである。ネットワークに流れている全パケットのデータ量は、大量である。そのため、全てのデータを収集する必要がない場合には、規則によって選択するためのフィルターを入れておく。そこから選択的にデータを取り出すことにより解析するデータを少なくすることができる。また規則は、パケットの内容と時間の項目によって条件を作って処理する。

3. 時間と規則による加算結果 (Counting)

一定時間、データを項目別に順次加えてゆく機能である。加算されたデータの結果がトラフィックの基礎データとなる。

4. 加算結果を解析 (Analysis)

加算した結果をパラメータごとにグラフや表にして解析を行なうことである。解析では、数学的なモデルとの近似の比較を行なったり、また定性的な解析を行なう。

インターネットのトラフィックを収集解析するためにネットワークモニター装置として汎用ワークステーションによるネットワークデータの収集解析システムを開発した [12]。このシステム、NOC(Network Operation Center)のバックボーンに接続してFDDIに流れている全パケットのヘッダー部分だけを記録して、そのパケットヘッダーが記録されたテープを順次読み出し解析し、最後にデータの収集結果を表やグラフに出すようにしている。

図5が、収集解析システムである。このシステムは、大きく分けて1)データ収集部、2)データ記録部、3)データ解析部のサブシステムからできている。データ収集部では、FDDIネットワークに流れている全データのパケットヘッダーを収集するため、汎用ワークステーションのカーネルに装備されているBPF(Berkeley Packet Filter)のインターフェイスを利用してプログラムの実装を行なった [11]。また、データ収集部から転送されたデータを一旦、ディスクに書き出して、その後、一定時間ごとにテープに書き込んでいる。テープ装置には、記

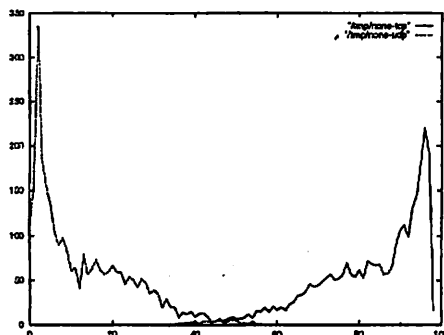


図 6: 全データと TCP 及び UDP の割合

憶容量が7GBの20連装テープ装置を使用して、プログラムにより自動的に7GBのテープを取り替えて使っている。データ解析部では、テープから収集したデータを読み出して、データの解析を行なっている。このようにテープに記録されている方式であれば、過去の同じ日時のデータを、方式をかえて何度でも解析することが可能となっている。またデータの解析は、ワークステーションにつけたテープ装置を使って行なった。

解析結果

アプリケーションの割合

1995年11月23日から12月12日までの20日間に収集したデータの解析結果を示している。図6から図8は、横軸がパーセントで表わされた比率で縦軸は頻度の表である。測定時間は、10分ごとになっている。図6では、トラフィックの全データのIPのバイト数のうち、TCP(実線)とUDP(破線)の比率とを頻度のグラフにして表わしている。縦軸に頻度とり横軸に全データの比率をとっている。つまりTCP(実線)だけに注目する

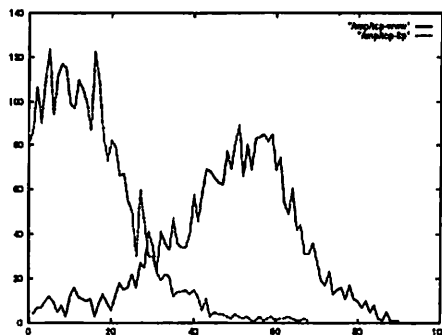


図 7: TCP と WWW 及び FTP の割合

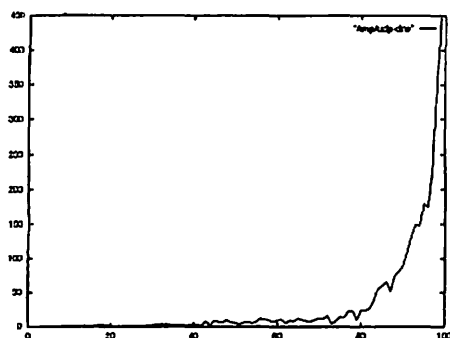


図 8: UDP と DNS の割合

と 97%前後にピークがある正規分布になっていることがわかる。また同じグラフで UDP(破線) だけに注目すると 2%にピークがある正規分布に従っている。つまり、TCP と UDP の比率は、それぞれピークが 97%と 2%で偏差を持った比率となっていることがわかる。また、図 7 は、TCP のうち、WWW(実線) と FTP(破線) の比率を頻度にして表わしたものである。FTP の頻度は、3%から 18%ぐらいに大きくなだらかなピークがあり、また、WWW は 58%ぐらいにピークがある大きな山である。図 8 は、UDP のうち DNS を抜き出して UDP との比率を頻度にグラフに表わしている。DNS は、UDP のうちで 99%を占めている。これは、UDP のトラフィックのうち、ほとんどすべてを DNS で占めている事を示している。

各アプリケーションごとの頻度

1996 年 3 月 12 日 0 時から 1 時までのトラフィックについて、FTP DATA と WWW のソースポートと目的ポートにおいて 1000 パケット以上あったホストを上位の 3 ホストにだけを表にして、それぞれパケット数とバイト数を示した。表 1 が、FTP DATA のソース及び目的

FTP DATA Source Port		
IP address	Packets	Bytes
128.149.70.66	61843	33719306
132.239.152.80	17247	9495706
198.112.44.100	5031	2753769

FTP DATA Dest. Port		
IP address	Packets	Bytes
128.183.10.141	31763	1270520
132.239.152.80	9316	372640
198.112.44.100	2849	113960

表 1: FTP-DATA のソースポートと目的ポート

WWW Source Port		
IP address	Packets	Bytes
202.241.3.30	196534	83950505
131.252.11.130	28039	15477528
192.50.77.195	11095	8033466

WWW Dest. Port		
IP address	Packets	Bytes
202.241.3.30	191019	11329075
131.252.11.130	17090	683600
192.50.77.195	9993	482373

表 2: WWW のソースポートと目的ポート

のポートの転送量の多いホストである。表 2 が、WWW のソース及び目的のポート別の転送量の多いホストである。FTP DATA であれば、ソースポートで上位は、get サブコマンドによって FTP サーバーから FTP クライアントへのデータが転送されていると考えられる。また目的ポートで上位は、put サブコマンドによって FTP クライアントから FTP サーバーへデータが転送されていると考えられる。

表 2 は、WWW のソース及び目的のポートにおいてパケット数が多い上位 3 つのホストのパケット数と転送量である。これをみると、ソース及び目的ポートの上位 3 つのホストは、同じである。

結論及び今後

以前の報告では、IP データ、TCP データ、UDP データ、ICMP に関してデータ量およびパケット数のそれぞれに述べた [13]。この場合、全データ及び TCP データにおいて時間の変化が顕著となり、UDP データでは、時間変化が見られないことがわかっている。また全データ及び TCP 時間変化は、一日のうち昼夜の変化、一週間のうち月曜日から金曜日と週末までの変化が規則があることがわかっている。本稿では、さらに各プロトコル間のデータ量の比率に関する解析を行なった。その結果、IP、TCP、UDP、WWW、FTP 及び DNS について、各プロトコルの間の関係を出した。また FTP DATA と WWW について一時間当たりのパケット数の上位をホスト別にして表わした。

今後、さらにトラフィックの流れの定義に従って、さらに系統的なデータの解析が必要であると考えている。

本研究を行なうにあたり省際ネットワークの運用管理を行なっている NTT 大手町省際ネットワーク NOC の方々及び NTT ソフトウェア研究所の方々には、FDDI バックボーンのトラフィック測定について色々とお世話になった。ここにお礼を申し上げる。

また本研究は、科学技術庁の「省際研究情報ネット

ワークの調査研究」として行なわれている。

参考文献

- [1] K. C. Claffy, H-W Braun, and G. C. Polyzos, A Parameterizable Methodology for Internet Traffic Flow Profiling, *IEEE JSAC*, Vol. 13, No.8, October 1995, 1995.
- [2] K. C. Claffy, H-W Braun, and G. C. Polyzos, Tracking Long-Term Growth of the NSFNET, *CACM*, 37(8), pp.34-pp.45, 1994.
- [3] K. C. Claffy, G. C. Polyzos, and H-W Braun, Traffic Characteristics of the T1 NSFNET Backbone, In *Proc. of Infocom 93*, 1993.
- [4] K. C. Claffy, G. C. Polyzos, and H-W Braun, Application of Sampling Methodologies to Network Traffic Characterization, In *Proc. of ACM SIGCOMM93*, 1993.
- [5] D. Sanghi, A. K. Agrawala, and O. Gudmundsson, Experimental Assessment of End-to-end Behavior on Internet, In *Proc. of Infocom 94*, 1994.
- [6] N. K. Groschwitz and G. C. Polyzos, A Time Series Model of Long-Term NSFNET Backbone Traffic, In *Proc. of ICC'94*, 1994.
- [7] V. Paxson and S. Floyd, Wide-Area Traffic: The Failure of Poisson Modeling, In *Proc. of ACM SIGCOMM94*, 1994.
- [8] W. E. Leland, M. S. Taqque, W. Willinger, and D. V. Wilson, One the Self-Similar Nature of Ethernet Traffic, In *Proc. of ACM SIGCOMM94*, 1994.
- [9] P. B. Danzig, K. Obraczka, and A. Kumar, An Analysis of Wide-Area Name Server Traffic, In *Proc. of ACM SIGCOMM92*, 1992.
- [10] J. A. Zinky and F. M. White, Visualizing Packet Traces, In *Proc. of ACM SIGCOMM92*, 1992.
- [11] S. McCanne and V. Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture, 1993 Winter *USENIX Conference*, 1993.
- [12] 串田, インターネットのトラフィックを測定及び解析するためのツールの設計及び開発, 情報処理学会マルチメディア通信と分散処理ワークショップ 1995 年 10 月, 1995.
- [13] インターネットにおけるトラフィック収集と解析, 情報処理学会マルチメディア通信と分散処理研究会 1996 年 2 月, 1996.