

インターネットにおけるトラフィック解析法の研究

3Aa-7

小松原 重之 鈴木 亮一 三上 博英

NTT ソフトウェア研究所

1.はじめに

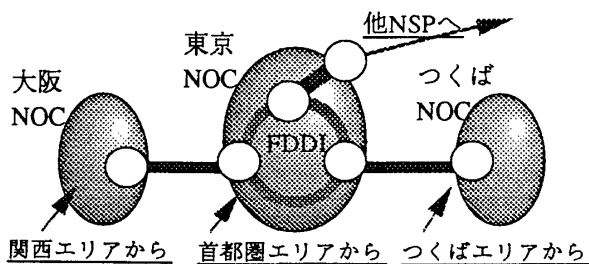
インターネットにおいてトラフィックを計測する意義は、大きく次の3つに分類できる。

- ・ネットワークのパフォーマンスを測る
- ・新しいアプリケーションと、そのネットワークへの影響を測る
- ・ネットワークの異常(あるいは正常性)を測る

個々の目的はさらに細かく分類できるが、基礎となるデータは同じものである。従って、目的に応じて、様々な表現がとれることが必要である。本稿では、省際研究情報ネットワーク¹⁾で我々の行っている解析アプローチを紹介する。

2.省際研究情報ネットワーク

省際研究情報ネットワーク(以下IMnet)は、国内外において、公的性格を有する研究機関を相互に接続するインターネットバックボーンである。以下に、IMnetの構成概略を示す。

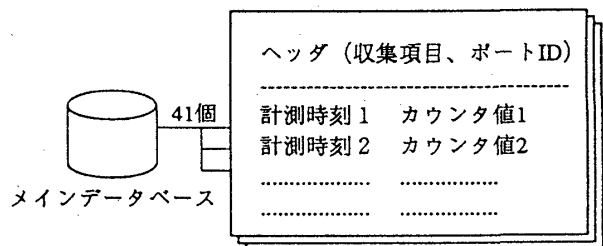


IMnetでは、転送パケット数、エラーパケット数、ユニキャスト/非ユニキャストパケット数などのMIB2²⁾で定義される11項目のデータを、ネットワークを構成する、全てのルータのポートにおい

て収集している。また同時に、FDDIリング上で、HTTPやFTPなどの15種類のアプリケーション別に、転送パケット数と転送データ量の2種類のデータを集計している。

3.データベースについて

我々は、これらの約40種類のデータを整備するために、メインとサブからなるデータベースを作った。メインデータの構造は以下のとおりである。



サブデータベースは、メインデータのヘッダ部に入る情報を管理するためのマトリクスである。

4.問題点

接続組織のNOCへの接続回線変更を例に、問題点を説明する。NOC側ルータの制限によって、元々收容されていたポートとは別のポートで收容することになったが、これは、トラフィックデータのヘッダにある収集項目、すなわちMIB-Indexが変更されることを意味している。

仮に、種別情報にMIB-Indexを用いたまま運用を続けた場合、その組織とNOC間のトラフィックデータは、2つのファイル(変更前と変更後)となって表現される。また、新旧のポートにさらに別の組織の收容があった場合には、トラフィックデータのファイルは、ある瞬間を境に2つの組織のデータが混在することとなる。

逆に、組織名などをキーとしてヘッダを構成した場合には、エラーレートをはじめとする、「ポート

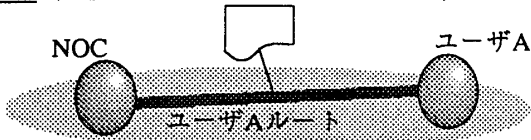
The methodology of analization of the Internet Traffic
Shigeyuki KOMATSUBARA, Ryoichi SUZUKI, and
Hirohide MIKAMI
NTT Software Laboratories

の信頼性」を解析するにあたり、同様の問題が生じて来る。リソースを長期的にモニタする上で、こちらも不可欠なデータの構造である。これは長期的変動を解析する上で、大きな問題となる。

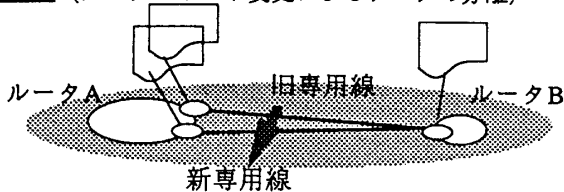
5. 解決法

以下にIMnetにおいて実装した、解決法を説明する。收容位置の繰り合わせによって、MIB-Indexとその示す接続先の変更が変更されるようなイベントは、ネットワークのトラフィックの「傾向」を解析するにあたり隠蔽される必要がある。それらを隠蔽したネットワークを論理網と定義した。一方、従来のリソースによって表現されるネットワークを物理網と定義した。以下の図は、そのモデルである。

論理網 (連続的な1つのトラフィックデータ)

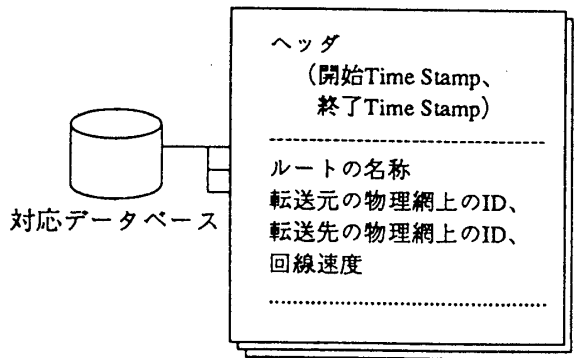


物理網 (ルータのポート変更によるデータの分離)



物理網上でのネットワーク構成の変化を、対応データベースで吸収することにより、論理網まで影響しないようにしている。

現在、対応データベースが実装しているデータの構造は、以下のとおりである。



6. まとめ

インターネットにおけるトラフィックに関するリ

ソースは、概ね固定的であるといえる。しかし、測定対象を「大規模かつ長期間」に設定する場合、それを静的に扱うことは難しい。

この問題に対して、対応データベースを用い、論理網を表現することにより、解析環境を作る方法について説明した。この結果、トラフィックデータによる、大規模なネットワークの記述を可能にした。

現在のシステムでは、2重化経路、機能分散型の複数の経路についてはうまく扱えない。しかし、バランシングアルゴリズムの評価や、極端な異速度回線接続の影響などを測るためには、ネットワーク上の全リンクを長期的に測定、解析し、複雑なトポロジーを扱えることが不可欠である。今後は、これらの目的を、十分に記述し得る論理網表現法に取り組む。

7. おわりに

データベースにアクセスするためのフロントエンドには、利用者の多様な環境を考慮しWWWクライアントを利用可能にしている。ネットワークの消費が著しい、昨今のアプリケーションの風潮からすれば、トラフィックをネットワークの利用者自身が、意識出来るような環境も必要ではないか、と考えている。

参 考 文 献

- 1) 鈴木亮一, 福田晴元, 三上博英, "省際研究情報ネットワークの構築について", 第51回全国大会2E-9, Sep 1995
- 2) K. McCloghrie, "Management Information Base for network management of TCP/IP-based internets: MIB: II", RFC1213, Mar 1991