

トラフィックパターンを用いた通信速度予測 Prediction of Network performance using time-series model of traffic

出石 大志† Hiroshi Izuishi
阿部 淳也† Junya Abe
堀 幸雄† Yukio Hori
今井 慈郎† Yoshiro Imai

1. はじめに

ネットワーク通信の技術は長足の進歩を遂げ、ここ数年はネットワークの高速化が進んでいる。また、ネットワークの高速化にともなって、LAN内にとどまらず、WAN間でも大容量データがやり取りされる傾向がみられる。オンデマンドTVなどの動画配信サイトの人気やオンラインゲームの普及も原因の一つと考えられる。

しかし、高速化には疎密があり、LAN環境とWAN環境が均一的に高速化されるのではなく、通信速度の遅いままの環境も存在するのが一般的である。従って、前世代のネットワーク設計が原因で通信遅延が発生するなどのケースもある。また、DoS攻撃などの外的要因でトラフィックが増大し、ネットワークに異常が発生する場合もある。その結果、ネットワーク利用に支障が生じる可能性もある。そこで本稿では、過去のトラフィックパターンを元に、現在のトラフィックパターンとの比較を行い、将来のトラフィックパターンを予測することで、将来期待できる通信速度を予測するための手法を提案する。

2. 既存技術について

多くの既存IDSはネットワーク上のパケットを取り込み、パケットの内容を解析することで自身の持つデータベースとのパターンマッチングにより不正パケットを検出する不正検出型である。この方式は、データベースにない未知のパターンの攻撃を検知することができないこと、トラフィックの増加により処理が追いつかず不正の検知率が低下してしまうことなどが問題である。DoS攻撃はトラフィックの増加によるサービス妨害を発生されるため、不正検出型IDSを使用するだけでは有効な対応策と言えない。

そこで、近年不正検出だけでは検出できない不正な行動を検出する異常検出型のIDSが増加している。異常検出型IDSは、通常とは異なるネットワーク上の振る舞いを検出することで未知の攻撃を発見するもので、サーバのシステム動作(ログイン時刻、使用コマンド)や、パケット内のIPアドレスやポート番号などを用いて統計的手法で判断し、異常を検出する。しかし、この方式だけでは、未知の攻撃には強いが、正常時に用いられているパケットでのDoS攻撃を検知することができない。つまりは、普段通信を行っているホストからのウィルスなどによるDoS攻撃には対応できないという問題が考えられる。

一方、トラフィックの予測に関する研究も多く行われており、様々な環境での応用が考えられている。しかし、これらのお大半がネットワーク障害の抑制や対策を目的としたネットワーク管理者向けに進められている研究であり、一般ユーザへの予測結果などの情報提示を目的としたものは少ない。今後のネットワークの混雑具合や通信速度を知ることがで

きれば、一般ユーザでの通信データのサイズを制限するなどの、通信の遅延を想定した対策を事前に立てることが可能であると考えている。本研究では、将来のネットワーク状況を予測し、管理者に加えて、一般ユーザへも情報提示することで環境の変化を理解してもらい、解決に協力してもらうことが重要であると考え、そのための対策を検討している。

3. システム概要

3.1 システム構成

本節ではトラフィック情報の取得からトラフィックの予測結果を返すまでのシステム全体について説明をする。今回提案するトラフィック予測のシステムの構成を図1に示す。

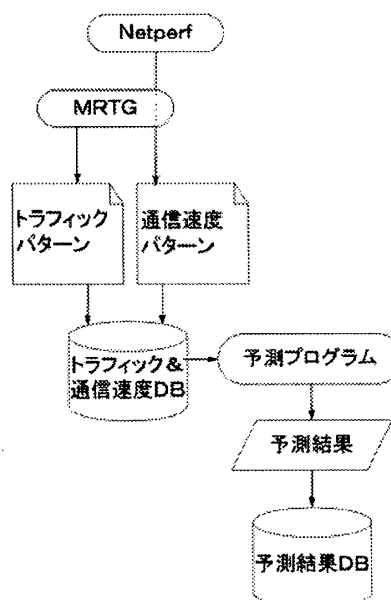


図1 システム構成図

トラフィックパターンはMRTG(Multi Router Traffic Grapher)を用いて常時5分間隔で測定を行っており、収集したトラフィックパターンのデータベースを作成する。また通信速度はNetperfを用いて測定を行っており、通信速度についてもMRTGを用いてグラフ化するため、MRTGからNetperfを実行させる形式とする。通信速度もトラフィックパターン同様に常時5分間隔で測定を行い、収集した情報のデータベースを作成する。作成されたデータベースのトラフィックパターンを用いて、観測した最新のトラフィックパターンと比較することでトラフィック予測を行う。予測されたトラフィックパターンは5章で提案する方法を用いてユーザへと提示される。またデータベースの作成を行い、後のトラフィック予測の精度評価などに用いる。

3.2 情報測定

本研究の目的は「トラフィックパターンを用いた通信速度予測」であり、本来は LAN 環境外の特定サイトまでの通信状況が分かることが望ましいが、WAN 環境において同様の手法でトラフィック情報、特定サイトまでの通信速度を測定することは外乱拡大の抑制などの観点から困難である。そこで、現在本研究では対象を香川大学の学内 LAN 環境に限定し測定を行っている。

測定を行ったトラフィックパターンは香川大学工学部内のギガスイッチにおける送受信トラフィック量の推移である。通信速度の測定区間は大学内の工学部と情報基盤が置かれている幸町内にある総合情報センターの間で行う。図2に測定対象となるネットワーク構成図を示す。

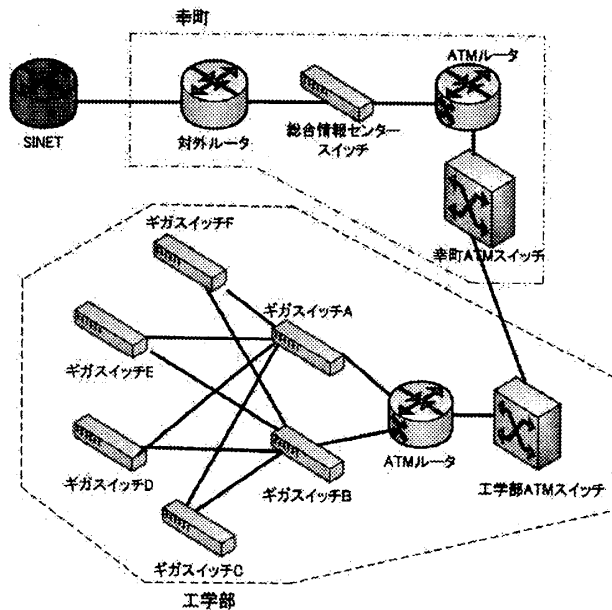


図2 香川大学のネットワーク構成

4. トラフィック予測手法

本節では、トラフィックパターンの予測に用いる手法について述べる。予測部分については、現在はまだ未実装部分であり、ここでは利用を検討中の手法について説明を行う。

まず1つは類似関数を用いた方法である。これはトラフィックパターンのデータベースを元に、最新のトラフィックパターンとパターンマッチングにて予測を行うもので、2つの式の相関関数を求めることで行う。数学的なマッチングを用いることで、高速な処理が期待できる。

他にはニューラルネットワークを用いてトラフィック予測を考えている。ニューラルネットは脳機能の特性を数学的にモデル化したものであり、自らのネットワーク構造を動的に変更することで最適な解を発見することができる。そのニューラルネットの中でもパターン認識に用いられるパーセプトロンの利用を考えている。パーセプトロンは、入力されたデータに対し、その答えが正解か誤りかによって出力結果を変化させる学習機能を持っています。しかし、ニューラルネットはその学習機能のために、処理に時間がかかってしまうという問題がある。また、場合によっては学習機能の低下による予測精度の低下も考えられる。

それぞれの手法の特徴について表1にまとめる。

表1 予測手法の特徴

	長所	短所
類似関数	高速な処理	未知なパターンへの対応不可
パーセプトロン	学習機能	処理の重さ

5. ユーザへの提示方法

2節でも述べたように、本研究では一般ユーザへの情報提示が重要であると考えており、いくつかの情報提示方法について検討中である。現在考えている提示方法とは以下の3つがある。

- ・ ウェブページへの埋め込み
- ・ 専用アプリケーション
- ・ ブラウザの拡張機能

「ウェブページへの埋め込み」については、情報提示専用ウェブサイトの作成や Blog などへの埋め込みを考えており、また、API 化することで個人のウェブページへの埋め込みも可能となる利点がある。「ブラウザの拡張機能」は、Firefox の extension や Google ツールバーなどのように、ウェブページの閲覧を行いながら、簡単に予測情報を知ることができる利点がある。

各方法の利害得失を考えると次のようになる。ウェブページへの埋め込みは新たなプログラムのインストールが不要で、ページアクセスのみで予測情報を知ることができる。逆にアプリケーションでは、インストールを行わなければならないという欠点があるが、提示情報や操作などの自由度が高く、拡張もし易いという利点がある。ブラウザの拡張機能では、ウェブページの閲覧を行いながら現在のネットワーク状況を知ることが可能である。しかし、アプリケーション同様インストールを行う必要があり、また、得られる情報が極端に限られてしまう欠点がある。このように、どの提示方法も一長一短であり、ユーザにとって情報を閲覧する際に何を重視するかが重要になってくるだろうと思う。

6. おわりに

本稿では過去のトラフィックパターンを用いて、現在のトラフィックパターンとの比較から、将来のネットワーク状況を予測することで、期待できる通信速度を予測する手法の提案を行った。本稿では、現在検討中のトラフィック予測手法およびユーザへの情報提示方法について述べた。

今後の課題としては、トラフィック予測部分の作成を行い、収集したトラフィックパターンを用いてのトラフィック予測を行うと共に、予測された結果の制度の評価を行っていきたい。また、ユーザへの情報提示方法について検討を行い、それによる作成を行う予定である。

参考文献

- [1] http://www.oecd.org/document/23/0,2340,en_2649_37441_33987543_1_1_1_37441,00.html (2007年7月アクセス)
- [2] <http://www.johotsusintokei.soumu.go.jp/index.html> (2007年7月アクセス)
- [3] 平石 陽太, 渡辺 一平, 宮内 充
「トラフィックパターン自動生成におけるDoS攻撃検知」
信学技報, vol. 104, no. 275, pp. 13-18, 2004年9月