トラフィックデータを活用した通信速度予測システム

出石 大志† 阿部 淳也† 堀 幸雄‡ 今井 慈郎‡
香川大学大学院工学研究科† 香川大学総合情報センター‡

1. はじめに

ネットワークの通信技術はここ数年で高速化が進んでいる．ネットワークの高速化に伴い，LAN内やWAN間でも大容量データでの通信がやり取りされるようになった．その背景には，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が考えられる[1]．

しかし，LAN環境がWAN環境に伴って高速化されていくのではなく，まだ高速化されていない環境も存在すると考えられる．このようなLAN環境における大容量データでのやり取りは，通信遅延を発生させる場合がある．また，トラフィック増大を起こすものとして，DoS攻撃などのような外部からの影響があり，ネットワーク障害の原因となる場合がある．

そこで本研究では，ネットワーク管理と障害予見を目的とし，過去と，現在のトラフィックパターンの比較を行い，将来のトラフィックパターンを予測するシステムの開発を行っている．本稿では，システム概要，トラフィック予測手法，ユーザへの提示方法について述べる．

2. 既存技術とその問題点

既存のIDSの多くは不正検出型である．これは，ネットワーク上を流れるパケットの内容を解析することで，予め登録されているシグネチャと呼ばれる侵入方法のパターンとマッチングさせることにより不正パケットを検出する．しかしこの方式は，既知のパターンの攻撃のみしか検知することができないこと，トラフィックの増加による処理能力低下のため不正侵入の誤検知が発生するなどの問題である．DoS攻撃によるトラフィック増加は通信障害を発生されるため，不正検出型IDSのみの使用では有効な対応策と言い難い．

そこで，不正検出だけでは検出不可能な行動を検出する異常検出型IDSが増加している．異常検出型IDSは，通常状態を記憶しておき，これに違反したネットワーク上の振る舞いを検出する．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基に統計的手法で判断し，異常を検出する．しかし，この方式は，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，トラフィック予測に関する研究も少なくないが，それらの多くはネットワーク障害の防止・対策を目的としたネットワーク管理者向けの研究であり，一般ユーザへの予測情報提示を目的としたものは少ない[2]．今後のネットワークの混雑具合や通信速度を一般ユーザに提示することにより，通信遅延を想定して通信データのサイズ制限を行うなどの，対策を立てることが可能であると思われる．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を行い，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

今回提案するトラフィック予測システムの構成を図1に示す．

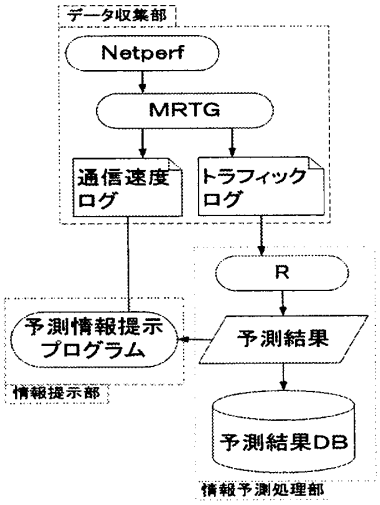


Fig.1 トラフィック予測システムの構成

A transmission rate prediction system using traffic data
Hiroshi Izuishi†, Junya Abe†, Yukio Hori‡, Yoshiro Imai‡
† Graduate School of Engineering, Kagawa University
‡ Information Technology Center, Kagawa University

トラフィックデータは 5 分間隔で MRTG (Multi Router Traffic Grapher) を用いて測定を行っている．また通信速度は Netperf を用いて測定を行っており，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データ同様に常時 5 分間隔で測定を行っている．トラフィックデータを用いて，測定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 節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「トラフィックデータを用いた通信速度予測」であり，本来は特定サイトまでのインターネットにおける通信状況が分かることである．しかし，本研究の手法で WAN 環境におけるトラフィック情報，特定サイトまでの通信速度を測定することはセキュリティ対策などの点から困難である．そこで，現時点では対象を大学内 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データは学部内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，学部と SINET 接続など学内ネットワーク基盤を担う総合情報センターの間で行う．

4.トラフィック予測手法

本研究は，「観測したトラフィックパターンと過去のトラフィックパターンが近似した場合，将来のトラフィックパターンも近似し，過去と同様の変化をする」という仮定に基づき予測を行う．

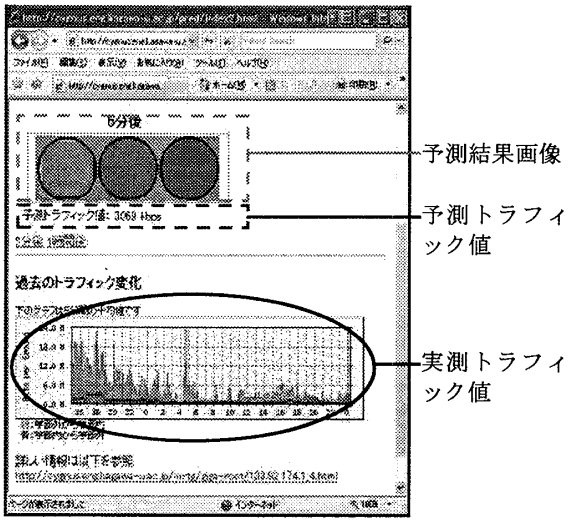
現在，予測手法には自己回帰モデル(以下 AR モデル)を採用している．AR モデルは，時刻 t で得られた時系列を X_t とし，式(1)によって得ることができる．$\alpha_i\,(i-1,\ldots,m)$ は自己回帰係数，ε は誤差である．

$$X_t = \alpha_1 X_{t-1} + \alpha_2 X_{t-2} + \ldots + \alpha_m X_{t-m} + \varepsilon \qquad (1)$$

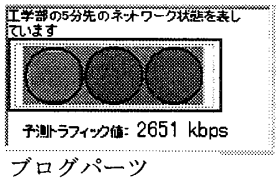
しかし，AR モデルを用いた予測では過去にない未知パターンの予測が困難であるため，パターン認識に優れているパーセプトロンの利用による予測を検討している．

5.ユーザへの情報提示

予測した将来のネットワーク状況を一般ユーザに通達するため，専用のウェブサイトとブログパーツの作成を行った．予測されたトラフィックデータは，一般ユーザ向けにネットワークの混雑状況が直感的に分かり易いよう，3 段階での情報提示を行う．また，管理者向けに予測値や，その時点でのトラフィック状況も分かるように過去 24 時間のデータも同時に提示している．ブログパーツでは，情報量に限りがあるため予測結果画像と予測値のみを提示する．



専用ウェブサイト



ブログパーツ

Fig.2 ユーザインターフェース

6.おわりに

本稿では過去と現在のトラフィックパターンの比較から，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．また，ユーザへの情報提示方法の概略について述べた．

今後の課題として，ニューラルネットを用いた予測の可能性を確認し，予測結果の精度の向上を行っていきたい．また，ユーザインターフェースにおいて，ブラウザの拡張機能としての開発や，提示情報の検討を行い更なる機能向上を行っていきたい．

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] 平石 陽太，渡辺 一平，宮内 充，トラヒ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