実計測トラヒックに統計数理モデルを適用した理論解析とその応用

１．研究代表者名

［国立情報学研究所］　阿部俊二

２．共同研究者

［統計数理研究所］　石黒真木夫、佐藤整尚
［国立情報学研究所］　松方純、計宇生

３．平成 18 年度の研究実績報告

3-1. 研究目標

［背景］

インターネットの使われ方が多様化するに伴い、そこに流れるトラヒックの性質が複雑化しており、従来の通信トラヒック理論を用いた解析手法の適用が難しくなってきている。最近では、ネットワークの混み具合、品質、性能を動的に感知し、最適な通信経路選択が要求される様なネットワークに高性能さが求められてきている。一方、DDoS アタックのように短時間で大量にトラヒックを発生させるネットワークサービスを妨害する行為を効果的に阻止する方法が強く求められているなど、ネットワークを安全かつ安心して使えることが求められている。これに応えるには、実際のトラヒックの計測から時々刻々と変化するトラヒックを旨く解析し予測できるような時系列解析手法が必要なると考えている。

［目標］

そこで、先ず実計測されたトラヒックの時系列解析モデルを明らかにし、これに基づいてネットワークの品質や性能を予測する時系列解析モデルの構築を行うこと、さらに DDoS アタックを広い意味での異常トラヒックと捉えて、その発生検出/予測のモデルの構築と、このアタックによるサービス妨害を予防・阻止するための危機管理運用手法の整理と提言を行うことを目標として進めている。

3-2. 平成 18 年度の研究成果（概要）

［H18 年度までの成果］

H17 年度の成果として以下が得られている。先ず、（１）実計測トラヒックの時系列モデルの検討をするために、現在のインターネットで使われている最高伝送路速度(10Gbps)までを範囲とする超高速ネットワークにおけるトラヒック計測の実現を学術ネットワーク（SINET）で行い、そのトラヒック計測環境の整備を行った。（２）この計測されたトラヒックに関する時系列解析モデルの検討を進め、計測系列トラヒックに中長期的な自己相関性があるため、マルチスケール FBM モデル、Fractional ARIMA モデル、トレンド成分とＡＲ成分等に分解して解析を行う Decomp 解析モデル等が適合可能性のあることを確認した。（３）DDoS アタックの発生メカニズムの調査と実計測された時系列トラヒックを比較し、異常トラヒックが発生した場合にそれが DDoS アタックなのかどうかを、アタックを受けるサーバ

一の入出力トラヒックの流量比から判定する一手法を考案した。

H18 年度は、H17 年度の検討結果を踏まえ、（１）効率的な時系列解析モデル検討を進めるためのトラヒック計測装置とネットワーク連携による解析処理系装置の整備、（２）中長期依存性を考慮した解析モデル（マルチスケール FBM、トレンド+AR 成分分解、Decomp 等）の有効性の明確化とこれらを応用した性能・品質予測モデルの検討と構築、（３）異常トラヒック予測検出からアタック検出を行う解析モデルの検討とサービス妨害の予防・阻止のための管理運用手法の整理と提言を目標に進めた。

H18 年度の成果は以下である。先ず（１）に関しては、H19 年４月から SINET の構成や機能が大幅に変更となることから、本ネットワーク構成や機能に対応した解析処理装置の仕様検討を進め、装置の整備を行った。（２）に関しては、0.1ms から 1ms の非常に短いサンプル時間による定常時系列トラヒックにマルチスケール FBM モデルを適用し、これを用いてルータバッファからパケットが溢れる品質評価する方法を明らかにすると共に有効性を示した。さらに、SINET の計測トラフィックを用いて、非定常な時系列トラヒックにトレンド+AR 成分分解モデルを適用した場合の検証を進め、特に長期的な予測に関して、予測値がかなり外れる場合がある事が分かった。SINET トラフィックには周期的な要素を含むため、これが予想外れの原因の一つと考えられる。周期要素に対応可能な季節調整を考慮した Decomp や三角関数を用いたモデルの検証も今後の課題として残る。（３）については、先ず、通信ネットワーク全体がどの様な状況にあるのかを把握することを狙いに、SINET の各通信ノードで計測したトラヒック時系列データを収集し、これらの相互相関解析からアプロチするためのモデル（多変量 AR モデル）の構築を行った。この統計的ネットワーク状況の把握から異常トラヒック検出やサービス妨害の予防・阻止のための管理運用手法の検討に発展させることが今後の課題である。

3-3. 今後の展開

今後は H18 年度の検討結果を踏まえ、次の目標で進める。（１）トラフィック時系列データの最適な予測モデルの明確化とこれを応用した通信ネットワークの性能や品質を予測する解析モデルの構築。（２）統計的アプローチによるネットワークサービス妨害の検出や、予防･阻止のためのネットワーク管理手法の明確化と提言。

（１）については、先ず H18 年度に残された課題の解決を通して、最適な予測モデルを明らかにする。さらに、予測モデルを用いて、動的な帯域管理と経路制御を取り入れた高性能なネットワークを実現するために必要となるネットワーク性能や品質を予測する解析モデルの構築をおこなう。

（２）については、先ず、ネットワークトポロジーとトラフィックの経路を考慮した適切な複数の計測点のトラフィック流量の時間変動に関する相互相関解析を、多変量 AR(MR,VAR) モデルを用いて行い、ネットワークサービス妨害(DoS/DDoS アタック)の発生メカニズムとトラフィック変動との関係を明らかにする。これらの結果を通して、アタック検出や、予防･阻止のためのネットワーク管理手法の提言としてまとめる。

４．成果発表実績

〔論文発表〕

＜学術論文＞

1. Yusheng Ji(計宇生), “Multi-scale Internet traffic analysis using piecewise self-similar process,” IEICE trans. Commun., Vol.E89-B, No.8, pp.2125-2133, 2006.

＜会議録＞

1. Fengxian Zhang and Shunji Abe, “In/Out trafficproportion based analyses for network anomaly detection,” 22nd APAN, July, 2006.
2. Ping Du and Shunji Abe, “Burst assembly method with traffic shaping for the optical burst switching network,” Globecom2006, Dec., 2006.

＜研究ノート＞

1. 佐藤尚整、“ネットワークトラフィックデータの解析、” 統計数理セミナー、９月、2006.