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．代表研究者名

［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、瀧澤由美

［国立情報学研究所］松方純、計宇生、長谷川亨

３．平成 17 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になると考えている。

[ねらい]

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を行うことをねらいとして進めている。

[H17 年度の目標]

（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とトラヒック計測環境の整備、（２）実計測トラヒックの時系列解析モデルの明確化、（３）異常トラヒック発生検出のアイディア抽出とその解析モデル検討を目標に進めた。

3-2. H17 年度の研究成果（概要）

（１）学術情報ネットワーク(SINET)に流れるトラヒックをリアルタイムに計測する環境の整備を行い、10Gbps の超高速ネットワークまでのリアルタイム計測を実現した。（２）実計測された時系列トラヒックの自己相関解析から長期依存性を有していることから、Fractal ARIMA モデルが時系列モデルの一つとして可能性があることを確認した。さらに、時系列データ解析ツールとして統計数理研究所で開発したトレンド成分と短期依存成分の分解から解析を行う Decomp モデル解析手法も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判定する一手法を考案した。DDoS アタックでは、アタックを受けるサーバーの入出力トラヒックの流量比（入力と出力の比）が極端に異なることから、入力と出力の比を計測して異常トラヒックを DDoS アタックとして検出するものである。

3-3. 今後の展開

（１）長期依存性を考慮したモデル（Fractional ARIMA, Decomp）の有効性を明確化し、これらモデルを応用した性能および品質予測モデルの検討と構築を進める。（２）さらに、効率的な検討を進めるために、トラヒック計測装置と Decomp をネットワークで連携した統合時系列解析処理系の整備を行う。（３）H17 年度で得られた DDoS アタック検出手法の有効性の検証を進めると共に、異常トラヒック発生検出の予測モデルの検討も進め、DoS/DDoS アタック検出の手法の実現を目指す。

3-4. 成果発表及び執筆論文

(1) Zhang Fengxiang and Shunji Abe, “A DoS/DDoS attacks detections scheme based on In/Out traffic proportion”, IEICE Technical Report IA2005-20, pp.7-11, Jan., 2006.

(2) Fengxiang Zhang and Shunji Abe, “A Heuristic Scheme to Distinguish Legitimate Traffic from Attack Traffic in Networks Anomaly Detection,” IEICE General Conference, March, 2006.

(3) 阿部俊二、松方純、計宇生、長谷川亨、石黒真木夫、佐藤整尚、瀧澤由美、“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、”融合研究シンポジュウム、情報・システム機構、３月、2006.