社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＳＭ－33　（７）
2004／5／13

フローを意識したトラフィック解析のための基礎実験

山本　成一[†a)]　　江崎　浩[†b)]

basic experiment of traffic analysys with consideration of flow

Seiichi YAMAMOTO[†a)] and Hiroshi ESAKI[†b)]

あらまし　近年, インターネットにおけるトラフィック解析では, 総転送量, 総パケット数など, パケットレベルの単一のカウンタを用いた解析が主流であった. 本研究では, 送信元から, 送信先までのパケットの一連の流れをフローとして扱うことで, よりオペレーショナルな情報の抽出が可能であると考慮し, そのフロー同定のための, 基礎的な解析を行い, フロー情報利用においての問題点の議論と考察を行った.

キーワード　トラヒック解析, フロー, サンプリング, ストリーム

1. まえがき

近年, インターネット利用の普及に伴い, 利用されるアプリケーション形態の多様化に伴い, インターネットトラヒックパターンは, 複雑なものになってきている.

従来では,web 閲覧, メール送受信など, 特定のサービスを提供するサーバと, ユーザの扱うクライアントが通信する, サーバクライアント型の通信が, インターネットトラヒックの大半を占めていた.

このため, その大半を占める, サーバクライアント型通信において, サーバ側でログを取ることで, インターネットトラヒックの傾向を知ることが可能であった.

しかし, 近年は, 利用されるアプリケーションの多様化が進み,IP 電話, インターネットメッセージングサービス, ファイル交換ソフトなどに代表される P2P 型アプリケーションの利用が多くなってきており, 従来のサーバログ分析のような手法では, インターネットトラヒック傾向の把握が困難になってきている.

このアプリケーションの多様化の他に, インターネットインフラの整備進行, 利用者のスタイルの変化, コンテンツの増大化などの要因により, インターネット利用の総トラヒック量も激しく増加してきている.

このため, インターネットトラヒックパターンの急激な複雑化が進んでいる.

本稿では, このトラヒックパターンの複雑化に対応した, 分析手法を検討し, その基礎的実験を行った. 2. では, 既存のトラヒックモニタリング手法を示し, 3. では, 本稿での実験について言及し, 4. にて, 考察を示し, 5. において, 今後の展開について述べる.

2. トラヒック測定

2.1 既存研究

既存のトラヒックモニタリング手法では, 測定ポイントに設置するエージェント, エージェントからの情報を収集するコレクタ(注1)が配置されることが多い. また, その特徴, 運用目的などにより定期チェック型, 特定トラヒック検知報告型, 一般トラヒック報告型として分別できる.

2.1.1 定期チェック型

コレクタが, 測定エージェントに対し定期的にチェックをかける方式. 測定エージェントが, 受動的に報告を行っている形と言える.

- mrtg

snmp エージェントと snmp コレクタからの構成されるシステム. コレクタから一定時間でポーリングを行い個々のインターフェースに対して, 単一のカウンタを持つのみであり, 多くの場合は, 総転送量の計測をしている.

コレクタ側では, ラウンドロビンデータベースを用

† 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The Universitiy of Tokyo
a) E-mail: yama@wide.ad.jp
b) E-mail: hiroshi@wide.ad.jp

(注1)：本稿では, 情報収集後, 解析もコレクタが行うものとする

い, データベースの肥大化を防いでいる為, 長期的な運用に向いている.

ただし, 一定時間でのポーリングを行っている為, ポーリング間隔において, 急激なトラヒック増加によるカウンタ溢れが発生した場合は, そのカウンタ溢れを検知することが出来ない.

また, ポーリング間隔は, 通常 5 分, 最短で 1 分であるため, リアルタイム監視には向かない.

2.1.2 特定トラヒック検知報告型

特定トラヒックを検知したときのみに, 測定エージェントから, コレクタへの報告が行われる方式. 測定エージェントが, 能動的に報告を行っている形と言える.

- ACL

ルータ, およびスイッチに含まれるアクセスコントロールリストシステム. 事前に検知対象の設定を行い, 特定トラヒックの転送制御を行う. 検知時に報告を行う機能を用いて, 遠隔の特定トラヒック検知が可能.

ただし, 事前に行う設定のため, 通過トラヒックのトレンド予想が必要なこと, 設定可能な検知対象数に制限あること, ルータおよびスイッチの基本的機能ではないため, 設計上, 比較的消費 CPU 能力が高いこと, が欠点として挙げられる.

- snmp trap

snmp の拡張. 上記の ACL と同様の機能を持つため, 長所, 短所も類似している. また, 特定トラヒック検知用に設計されているため, 消費 CPU 能力は,ACL ほど高くならなず, 検知時の処理においても, 複雑な処理が可能である. しかし,ACL と同様, 通過トラヒックを想定した設定が事前に必要となる.

- IDS

侵入検知システム. 上記の ACL などの検知内容に加え, パケットのバイト単位処理など, 高度な機能を持つ. その反面, 事前に, 多くの複雑な項目について設定が必要であり, 熟練度を要する, という問題がある.

2.1.3 一般トラヒック報告型

トラヒックのサマリ, またはトラヒックの一部などを, 測定エージェントからコレクタへ能動的に報告する方式.

上記の特定トラヒック検知型との違いは, すべてのトラヒックに対し, 能動的な報告が行われる点である.

- netflow [1] [2] [3]

エージェント側に, ある一定時間のトラヒックパターン, たとえば, 同一な, 送信元アドレス, ポート番号, 受信先アドレス, ポート番号, プロトコル番号の組をフローと認識し, フロー毎のカウンタ値を一定時間毎, または, 一定のカウンタ値になると報告を行うシステムである.

特定トラヒック検知型と異なり, すべてのトラヒックに対して報告が行われるため, 事前に行う設定は極めて少ない.

しかし, そのフロー識別, およびカウンタ保持のため, 大量のトラヒックを扱う場合は, 消費 CPU 能力, および, 消費メモリ量の増加が, 主要な処理である, ルーティング, およびスイッチング処理への影響を与えてしまうこととなる. また, 報告間隔が 5 分程度, と比較的長く, リアルタイム監視には向いていない.

- sflow [4]

上記 netflow と類似して, 能動的に報告を行うシステムだが, すべてのトラヒックに対しては報告を行わず, パケット単位のカウンタを用いて, 一定量のカウンタ増加に伴い, パケットのヘッダ部分および, ペイロードの一定長を直ちに報告するシステムである. コレクタ側で, 報告パケットを受け取った後, データ解析を行うシステムとなる. サンプリングを行った後, 直ちに報告を行っている為, 大量のトラヒックを扱う場合でも, 比較的, 消費 CPU 能力, 消費メモリ量の増加は発生せず, また, 他の測定手法と比較して, リアルタイム監視に向いているといえる.

一方, サンプリングを行っている為, 計測対象に正確に合致した測定結果を得る事はできない, という問題がある.

- aguri [5]

すべてのトラヒックに対し, ある時間単位で, 送信元又は, 受信先の IP アドレスを集約して記録するシステム. 集約により, 長期観測におけるデータ量の増大を緩和することができる. データ更新間隔の仕様のため, リアルタイム監視には向かない.

また, このシステムは, 単体で動作するため, エージェント, コレクタ, それぞれの機能がされたシステムと考える事が出来る.

2.1.4 そ の 他

- tcpdump [6]

トラヒックをそのまま記録する事が可能だが, その反面, 記録量は直ちに膨大な量となるため, 長期監視には向いていない. 但し, 短時間での詳しいトラヒック監視には向いている.

2.2 必 要 条 件

単一カウンタからの転送量や, 限られた数の特定ト

ラヒック検知のみでは, 多様化したトラヒックパターンの把握は困難である. よって, フローを意識したトラヒックモニタリング手法が必要となる.

また, 近年は 10 ギガビットイーサネット技術など, 計算機の処理能力を越えたトラヒックを流すことができる技術の利用が増加していることを考慮すると, 高速ネットワークに対応した測定手法が必要となる.

以上の要件を満たす測定手法としては, sflow, 又はこれに類似した, サンプリングを行いつつ, フロー情報を把握できる技術が必要となる.

2.3 sflow の利用

sflow は,flow という言葉が含まれてはいるものの, エージェントから報告される情報にはフロー情報は含まれない. そのため, 報告情報を受け取ったコレクタがフロー情報を構成し, 解析を行う必要がある.

N.Duffield らは数学的手法に基づき, サンプリングで取り落としたパケット情報を推定する手法, およびフローの長さを推定する手法を提案している. [7], [8]

また,IETF psamp wg [9] では, パケットサンプリング, IETF ipfix wg [10] では, フロー情報の取扱い, について議論されているが, 現在公開されている sflow 対応コレクタは, 一般的に netflow との互換性を意識したものであり, サンプリングを意識した, フロー識別機能や, 解析機能が不十分である.

我々はサンプリングおよび, フロー情報管理において, 十分な機能を持つコレクタ作成を計画した. この基礎情報収集のため, フロー識別を目的とした基礎実験を行った.

3. 基礎実験

3.1 実験構成

我々は, ライブ!ユニバース(注2) の協力を得て, 日食中継イベント LE2003 において,2003 年 11 月 24 日 6 時から 9 時の間, ストリーミングトラヒックを観測した.

外乱を最小にするため, ストリーミングサーバ, エージェント, コレクタと, コレクタのバックアップ用として,tcpdump を行うマシンを, IIJ-MC(注3) データセンタに一括して設置した. また, ストリーミングサーバの設定の下, ストリーミングサーバから, クライアントへ向かうパケットのみを取得した.

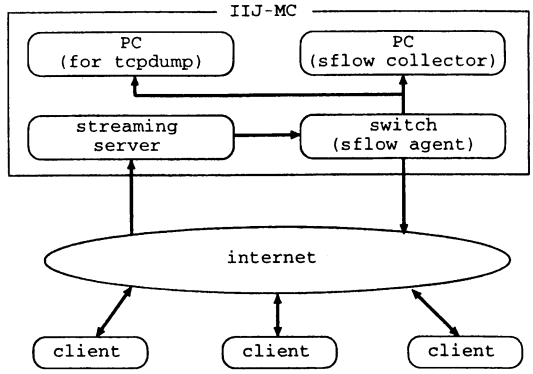

図 1 LE2003 での実験トポロジ

本稿では, 簡単のため, フロー定義を, 送信元アドレス, 送信元ポート番号, 受信先アドレス, 受信先ポート番号, プロトコル種別 (TCP,UDP, その他), プロトコル番号が一致するパケットの集団を同一のフローとし, 時間変化において, 異なるフローとしては扱わないこととした.

また, フローとしての連続性が高いと思われる動画ストリーミングを, 測定対象とした.

なお, サンプリングはパケットカウンタを用い, サンプリングレート N の場合は,N 個のパケットから 1 個のパケットを採取する方式でサンプリングを行った.

使用機器, ソフトウエア

- ストリーミングサーバ(注4)

network appliance netcache C1100

- sflow エージェント

Foundry networks FastIron4802

- sflow コレクタ用マシン,tcpdump 用マシン

JCS vintage, CPU:Pentium3 850MHz,RAM: 256MB, HDD 60GB

- sflow コレクタソフトウェア

sflowtool 改造版 + mysql 4.0.18-5

- ストリーミング用規格

Microsoft WMT9(注5),Real Networks RealVideo,Apple Quick Time , 各 high rate(384kbps),low rate(64kbps)

3.2 実験結果

測定時間 約 2 時間, テキストベースでの sflow 出力として,20GB のデータベースを得た.

(注2) : 天文および宇宙科学に関する現象をイベントやネットワークを通じて広く世界に紹介し, 社会に貢献することを目的とする団体, http://www.live-eclipse.org/

(注3) : 株式会社アイアイジェイメディアコミュニケーションズ

(注4) : LE2003 では, 正確には負荷分散のため, ストリーミングキャッシュサーバを利用した. しかし, 本稿に関する要件では, ストリーミングサーバと表現しても問題無いと判断した.

(注5) : Windows Media Techonology

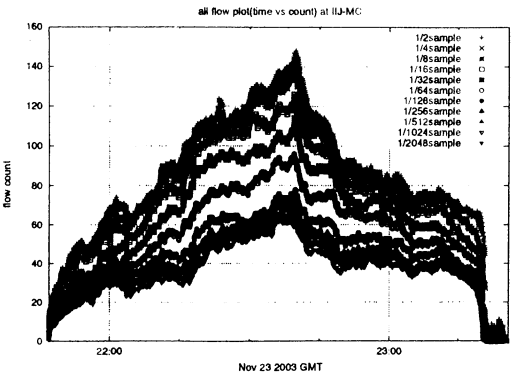

図 2　サンプリング頻度毎に認識されたフロー数変化

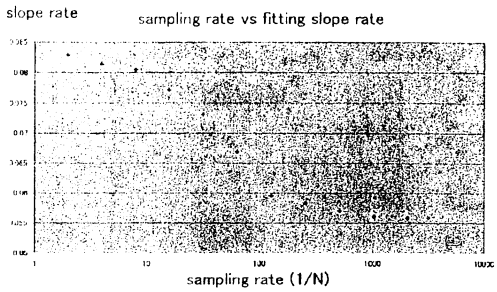

図 4　線形回帰推定における傾き変化

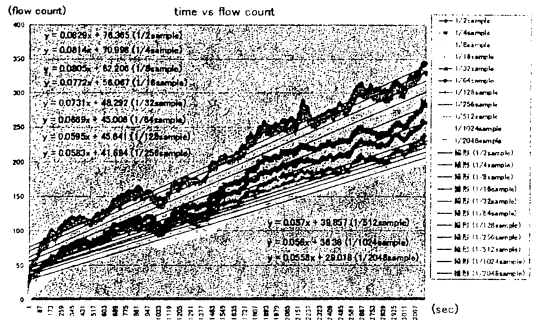

図 3　フロー数変化に対する線形回帰推定

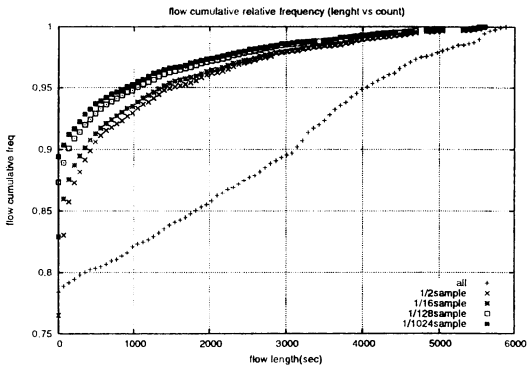

図 5　フロー時間を対象とした累積度数分布

得られたフロー情報, および, ストリーミングサーバのログから,

サンプリング頻度毎に認識されたフロー数変化 図 2, フロー数変化に対する線形回帰推定 図 3, 線形回帰推定における傾き変化 図 4, フロー時間を対象とした累積度数分布 図 5, を作成した. なお, 図 5 では, 度数区間幅 k は, サンプル数およそ n=6000 より, スタージェスの公式を用いた場合, k=13 となり, 分布が密になりすぎた為, 目安として n の平方根を用い,k=70 とした.

4. 考　　察

図 2 より,1/2 から,1/2048 までサンプリングレートを変化させても, フロー数の増減変化が似ていることより, サンプリングによるトレンド把握は可能であることが分かる.

次に, 図 2 の一部において, 線形回帰推定を行い, サンプリングレートと回帰推定においての傾きを見ると, サンプリングレートが 1/32 から 1/128 へ変化する部分が急激に変化していることが分かる. これは, 図 2 においても, 各サンプリングレート間で, 大きく間があいていることからも認識できる.

図 5 において, サンプリングレートと, フロー時間の変化を見ると, ストリーミングサーバの正確なログより, フローで,70 秒以上の長さを持つものは, ほぼ一様に分布していることが分かる. この一様分布の状態において, サンプル頻度を下げる, つまり 1/N の N を大きくすると, フロー時間を短く判定することが分かる. また, この図においても,1/16 から 1/128 の区間において, 各サンプリングレート間で大きく間が空いていることから, 本実験の環境では, 1/16 から 1/128 の確率で, 何らかの偏りが生じていることが予想される.

5. むすび

ネットワークトラヒックパターンの複雑化, および高速化していく中で, トラヒック計測技術もまた, その複雑化, および高速化に対応する必要がある.

本稿では, パケットサンプリングを行った上で, フロー定義を行い, フロー認識とサンプリングの関係に着目した上で, 本環境においての, サンプリングレートの変化点を指摘した. 今後は, パケットサイズの分布, および, ポート番号を反映した状況に応じてのフィルタ利用を考慮して, より詳しい解析を行う予定である. また, ストリーミングに限定せずに, 多くのアプリケーション利用を反映した複雑なフローに対しても解析を行う予定である.

文　献

[1] "Netflow" http://www.cisco.com/warp/public/732/Tech/nmp/netflow/

[2] Jurgen Quittek, Tanja Zseby, Georg Carle, Sebastian Zander, "Traffic Flow Measurements within IP Networks, The 2002 International Symposium on Applications and the Internet (SAINT 2002), February 2002

[3] Cristian Estan, Stefan Savage, George Varghese. "Automated Measurement of High Volume Traffic Clusters." Internet Measurement Workshop 2002 , November 2002

[4] "sflow" P. Phaal, S. Panchen, N. McKee RFC3176, September 2001

[5] Kenjiro Cho, Ryo Kaizaki, Akira Kato, "AGURI: An Aggregation-Based Traffic Profiler", QofIS2001, September 2001

[6] "tcpdump" http://www.tcpdump.org/

[7] Nick Duffield, Carsten Lund, Mikkel Thorup, "Properties and Prediction of Flow Statistics from Sampled Packet Streams", ACM SIGCOMM Internet Measurement Workshop 2002, November 2002.

[8] Nick Duffield, Carsten Lund, Mikkel Thorup, "Estimating Flow Distributions from Sampled Flow Statistics", ACM SIGCOMM Internet Measurement Workshop 2003, August 2003

[9] "IETF psamp wg" http://www.ietf.org/html.charters/psamp-charter.html

[10] "IETF ipfix wg" http://www.ietf.org/html.charters/ipfix-charter.html

(平成 xx 年 xx 月 xx 日受付)

山本　成一

平 13 東大・工・計数卒. 平 15 同大大学院情報理工学系研究科修士課程了. 同年同大大学院情報理工学系研究科博士課程進学. ネットワーク運用に従事しつつ, ネットワークトラヒック計測の研究に従事. WIDE プロジェクトメンバ.

江崎　浩　(正員)

昭和 60 九大・工・電子卒. 昭 62 同大大学院修士課程了. 同年 (株) 東芝入社. 平 2 米国ベルコア社客員研究員, 平 6 米国コロンビア大客員研究員. 平 10 東大大型計算機センター (現, 情報基盤センター) 助教授, 平 13 同大大学院情報理工学系研究科助教授, 現在に至る. 工博. 高速インターネットアーキテクチャの研究に従事.WIDE プロジェクト運営協議会委員.JGN 運営委員会委員. 平 6 本会学術奨励賞, 平 9 電気通信普及財団奨励賞, 平 10 日刊工業新聞十大製品受賞