超高速ネットワークにおけるトラヒック測定分析技術

川原　亮一，森　　達哉，石橋　圭介，阿部　威郎

本稿では，超高速ネットワークにおけるトラヒック測定分析技術として，サンプルパケットのみを用いてトラヒック制御・品質管理に有用な統計情報を推定する手法を二つ紹介する．まず，回線帯域の占有率が大きいユーザを特定する手法について述べる．本手法は，帯域占有率の大きいユーザが他の一般ユーザの通信を圧迫している場合に，そのようなユーザを迅速に切り分けて制御することを可能とする．次に，パケットサンプリングにより抽出されたユーザのみの挙動から元のユーザ全体の品質劣化を検出する方法について述べる．また，実測データ分析を通じて各方式の有効性を検証した結果についても報告する．

キーワード：超高速ネットワーク，トラヒック測定，パケットサンプリング

1．はじめに

通信ネットワークを適切に運用するには，ネットワークを流れるトラヒックや通信品質を測定・管理することが不可欠である．近年，回線速度の高速化に対してスケーラブルなトラヒック測定を可能とする技術としてパケットサンプリングが注目されている[1]．パケットサンプリングは，例えばN個に1個のパケットを周期的に参照し，サンプルされたパケットのみを分析することにより，測定分析に必要とされる処理を軽減させる．ここで，サンプルパケット情報のみを用いていかに必要な情報を精度良く推定するかが問題となってくる．本稿では，サンプルパケット情報からトラヒック制御・品質管理に有用な統計情報を推定する手法について，著者らのこれまでの検討結果を二つ紹介する．まず，回線帯域の占有率が大きいユーザを特定する手法[2]について述べる．本手法は，そのようなユーザが他の一般ユーザの通信を圧迫することを回避できるよう，帯域占有率の大きいユーザを迅速に切り分けて制御あるいは分離することを可能とする．次に，パケットサンプリングにより抽出されたユーザのみの挙動を把握して，元のユーザ全体の品質劣化を検出する方法[3]について述べる．また，実測データ分析を通じて各方式の有効性を検証した結果についても報告する．

かわはら　りょういち，もり　たつや，あべ　たけお
NTTサービスインテグレーション基盤研究所
〒180-8585 武蔵野市緑町3-9-11
いしばし　けいすけ
NTT情報流通プラットフォーム研究所
〒180-8585 武蔵野市緑町3-9-11

2．高トラヒックユーザフロー特定手法

2.1 エレファントフロー

本稿では，同一の（発信元IPアドレス，着信先IPアドレス，発信元ポート番号，着信先ポート番号，プロトコル番号）を持つパケット群をユーザフロー（あるいは単にフロー）と定義する．このフローの定義に基づいて，データを分析することにより，ユーザレベルのトラヒック特性（例えば，どのユーザがどれ位のトラヒックを発生しているか）を把握することができる．フローjのパケット数X_jの分布を実測データから分析した結果を図1に示す．実測データとして，2.4 Gbps回線上で10^7個のパケットをキャプチャしたトレースを用いた（トラヒック量は平均約500 Mbps）[2]．これより，X_jの分布はほぼべき乗の形で減衰し，裾野が重い性質を有することが分かる．様々なインターネット回線上において，このようなトラヒック特性を有することが報告されている．このデータ

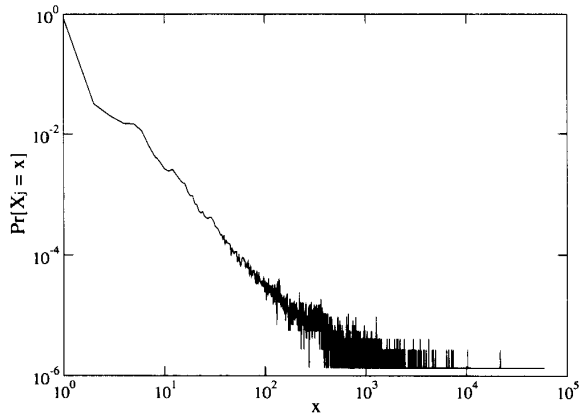

図1　フロー当たりのパケット数分布

において，総フロー数は737,780であり，そのうち，$X_j \geq 10^4$であるフロー（エレファントフローと定義する）の数は167本であり，これらごくわずかなフローによるトラヒック量の総計は全体の59.3%を占める．

2.2 エレファントフロー特定手法

サンプルパケットから帯域占有率の大きいフロー(エレファントフロー）を特定する手法を提案する．パケットサンプリングを行うと，少数パケットで構成される大多数のフローは無視されるが，エレファントフローはサンプルされる確率が高いことを利用する．ここでは，あるフローについてサンプルされたパケット数が$\hat{y}$以上であるとき，エレファントフローと判定する方法を考える．このとき，サンプルされたフローがエレファントフローではない確率をある一定値以下に抑えるようにしきい値$\hat{y}$を決定する必要がある．次ではこのしきい値決定方法について説明する．

N個のパケットを母集団とし，母集団からランダムにn個のパケットをサンプルする場合を考える．また，n個のサンプルパケットの内，フローjからとりだされたパケットの数をY_jとする．あるフローjの母集団におけるパケット数が$X_j=x$であるという条件のもとで，サンプリングによってとりだされるフローjのパケット数が$Y_j=y$である確率は，次式の超幾何分布であたえられる．

$$\Pr[Y_j=y|X_j=x]={}_xC_y\,{}_{N-x}C_{n-y}/{}_NC_n \tag{1}$$

サンプリングによってとりだされたフローjのパケット数が$Y_j \geq y$という条件のもとで，そのフローjの母集団におけるパケット数が$X_j \geq x$である確率は，

$$\Pr[X_j \geq x|Y_j \geq y] = \frac{\sum_{i=x}^{N}\Pr[Y_j \geq y|X_j=i]\Pr[X_j=i]}{\sum_{i=1}^{N}\Pr[Y_j \geq y|X_j=i]\Pr[X_j=i]} \tag{2}$$

と計算できる．$N, n, x, \Pr[X_j=i]$を与え，次で定義されるfalse positive ratio (FPR)（誤ってエレファントフローと判定する確率）をϵ(e.g., 0.05)以下とするようなyの最小値$\hat{y}$を求め，それをしきい値として用いれば，誤判定率をϵ以下に抑えてエレファントフローを検出できる．

$$\mathrm{FPR}(y) := 1-\Pr[X_j \geq x|Y_j \geq y] \tag{3}$$

2.3 評価結果

$N=10^7, x=10^4$とし，図1に示した実測データの$\Pr[X_j=i]$を用いて，式(3)を$\epsilon=0.05$以下とする$\hat{y}$を求めると，$n=10^4$のとき$\hat{y}=13$, $n=10^3$のとき$\hat{y}=4$であった．それらの値を用いて提案方式を実測データに対して適用したときの評価結果を表1に示す．ここで，$f=n/N$はサンプリングレート，$\hat{n}_e$はサンプリングによって$\hat{y}$以上のパケットが検出されたフロー数，n_eはそれらのフローのうち実際にエレファントフロー（i.e., 10^4個以上のパケットからなるフロー）であった数を表す．これより，FPRを理論値程度に抑えられていることが確認できる．また，false negative ratio (FNR)（エレファントフローを見逃す割合）についても評価した．FNRは，$\mathrm{FNR}=1-n_e/N_e$（N_eは真のエレファントフロー数で167）と定義される．表1より，fが小さくなるとFNRが大きくなることが分かる．つまりトラヒック測定にかかるコストと特定精度はトレードオフの関係にある．ただし，トラヒック制御の観点からは，低いサンプリングレートで検出されたエレファントフローであってもその情報は有用であると考えられる．なぜなら，検出されたフロー（$n_e=38$フロー）の多くはエレファントフローの中でも特にフロー当たりのパケット数の多いフローであり，これらフローによるトラヒック量は全体の約1/5以上を占めているため，これらフローを制御対象とするだけでも制御の効果は期待できると考えられるからである．

表1 エレファントフロー特定精度評価結果

f	$\hat{n}_e$	n_e	FPR	FNR
10^{-3}	134	127	0.053	0.240
10^{-4}	38	38	0.000	0.772

3. フローレベル品質劣化検出法

本節では，パケットサンプリングにより抽出されるフローの統計情報から，ユーザフローレベルの品質劣化を検出する方法を提案する．なおここでは，通信品質としてTCPのフローレート（＝フローサイズ/フロー持続時間）を扱う．フローレートはユーザが体感するファイル転送速度に相当し，フローレートが低下することが通信品質が劣化していることになる．

提案手法は，(i)パケットサンプリングで抽出されるフローが高レートフローになりやすく，(ii)リンク輻輳時にはレートの高いフローから先に品質劣化が生じる，という二つの特性を利用する．これら特性(i), (ii)を用いれば，パケットサンプリングで抽出されたフローのみの挙動を把握することにより，フロー管理に必要とされる処理を軽減しつつ，フロー全体のうち輻輳に敏感なフロー（高レートフロー）の品質劣化を検出することが可能となる．

3.1 フロー特性分析

前に述べた二つの特性について，実測データを用いて示す．ここでは，ある企業LAN～ISP間の17 Mbps回線において，2003年8月の平日数日間，全パケットヘッダをキャプチャしたデータを用いた．

図2に，ある15分間におけるフローサイズとフローレートの散布図を示す（フロー数は111,086本であった）．これより，フローサイズが大きい程，フローレートが大きくなる傾向にあることがみてとれる（同様の結果が文献[4, 5]で詳細に述べられている）．したがって，サンプルされるフローはサイズの大きいフローになりやすいこと[2]と併せれば，サンプルされるフローレートは高めになると予想される．

図3に，f^{-1}個（f^{-1}=1, 10, 100, 1000）に1個の周期でパケットサンプリングしたときに抽出されたフローのフローレート分布を示す．これより元のフローレートに対し（図中f^{-1}=1の結果），サンプリングするとフローレートが高くなっていること（i.e., 特性(i)）が確認できる．

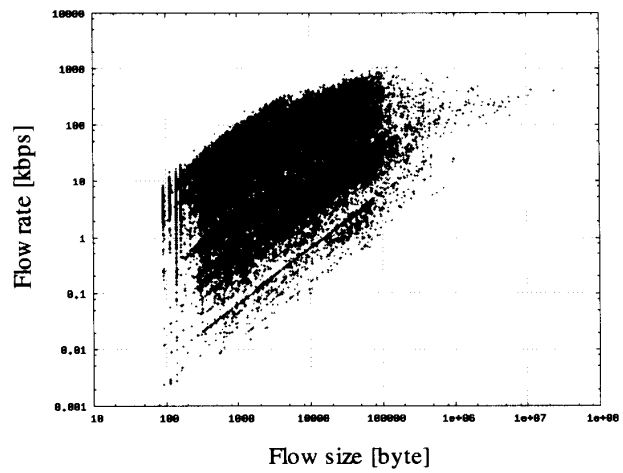

図2 フローサイズvsフローレート

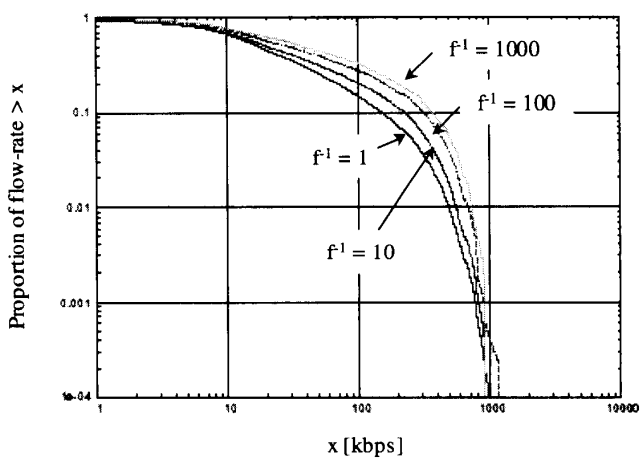

図3 サンプリングしたときのフローレート分布

次に特性(ii)について，実測データを用いて示す．図4に，ある平日8：30～18：00のリンク使用率，およびフローレートがr_{th}（r_{th}=10, 100, 1000 kbps）を超えた割合の時系列データ（15分間隔）を示す．これより，リンク使用率が1に近くなりリンクが輻輳すると，1,000 kbpsを超える割合はリンク使用率が低い時間帯に比べて非常に小さくなるのに対し，10 kbpsを超える割合はほとんど変わらないことが分かる．つまり，リンク輻輳時には転送可能レート（リンク非輻輳時のレート）の高いフローから先に品質劣化が生じている（この現象は，TCPフロー制御による帯域配分がmax-min公平性と呼ばれるものに従うと考えられることを用いて説明できる[3]）．したがって，リンク非輻輳時のレートの高いフローの方が，輻輳に敏感に反応して品質劣化を生じ，かつ，その劣化度（＝リンク非輻輳時のレート/リンク輻輳時のレート）も大きくなる．

3.2 提案方式

Step 1) 周期τごとに区間$((i-1)\tau, i\tau]$でのリンク使用率$\rho(i)$を測定する．また，サンプリングレートfでパケットを抽出し（i.e., f^{-1}個の到着パケットに対し1個のパケットを抽出），そのパケットが属するフローkのレート$F_k(i)$を求める（$F_k(i)$の推定方法は文献[3]参照）．τ時間経過したら，サンプルされた各フローのレートを用いて，平均フローレート$\bar{F}(i)$を

$$\bar{F}(i)=\sum_{k=1}^{N_f(i)} F_k(i)/N_f(i) \tag{4}$$

により求める（ここで，$N_f(i)$はサンプルされたフロー数）．

Step 2) 品質劣化が起こり得ないと考えられる使

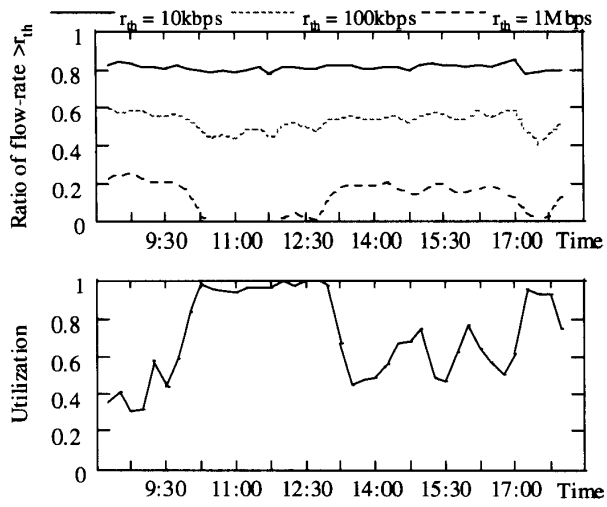

図4 フローレートがr_{th} kbpsを超える割合

用率に対するしきい値(ρ_0)(e.g., 0.6)を定めておき，$\rho(j)<\rho_0$を満たす組($\rho(j), \bar{F}(j)$)を抽出し（組数をmとおく），

$$F_{avg}=\sum_j \bar{F}(j)/m \tag{5}$$

とする．ここで，F_{avg}はリンク非輻輳時のフローレートを意味する．

Step 3) F_{avg}と，あらかじめ定めた品質劣化許容度γ(e.g., 0.3)を用い，現時点$n\tau$のフローレート$\bar{F}(n)$が

$$\bar{F}(n)<(1-\gamma)\times F_{avg} \tag{6}$$

であれば，品質劣化状態にあるとして検出する．

この方式では，リンク非輻輳時のフローレートF_{avg}を品質が維持できているときの基準フローレートとし，それと比べて現在のフローレート$\bar{F}(n)$が予め定めた品質劣化許容値ϵよりも下回ったら品質劣化として判定している．

3.3 評価

まずサンプルされたフローレートの平均と，元のフローレートのそれの挙動を比較した．図5に，f^{-1}個に1個のサンプリングを実施したときのフローレート(15分間隔）の時系列を示す．併せて，リンク使用率も示す．これより，元のフローレート（i.e., $f^{-1}=1$の場合）が劣化している状況をサンプルされたフローレートから推定できることが期待される．

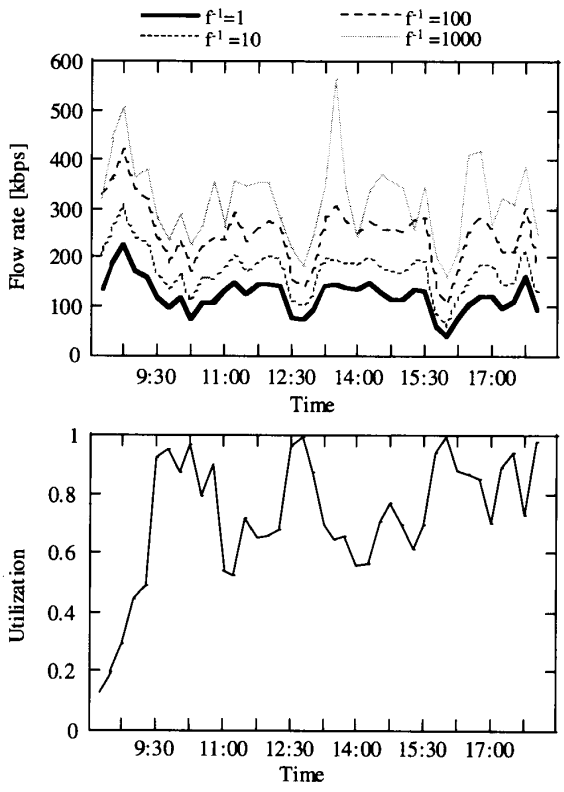

図5 サンプルされたフローレートの振る舞い

図6に，8：30～18：00における平日5日分（測定周期は15分で，測定回数は195回）の平均フローレートとリンク使用率の散布図をプロットした．ここでは，元のフローレートと$f^{-1}=10, 100, 1000$でサンプリングしたときのフローレートを比較した．これらの図からも，元のフローレートとサンプルされたフローレートは値自体は一致しないが（高めになる），サンプルされたフローレートから元のフローレートの劣化を検出できることが期待される[1]．

次に，図6のデータを用いて，提案方法の検出精度を評価した．検出精度の評価においては，サンプリン

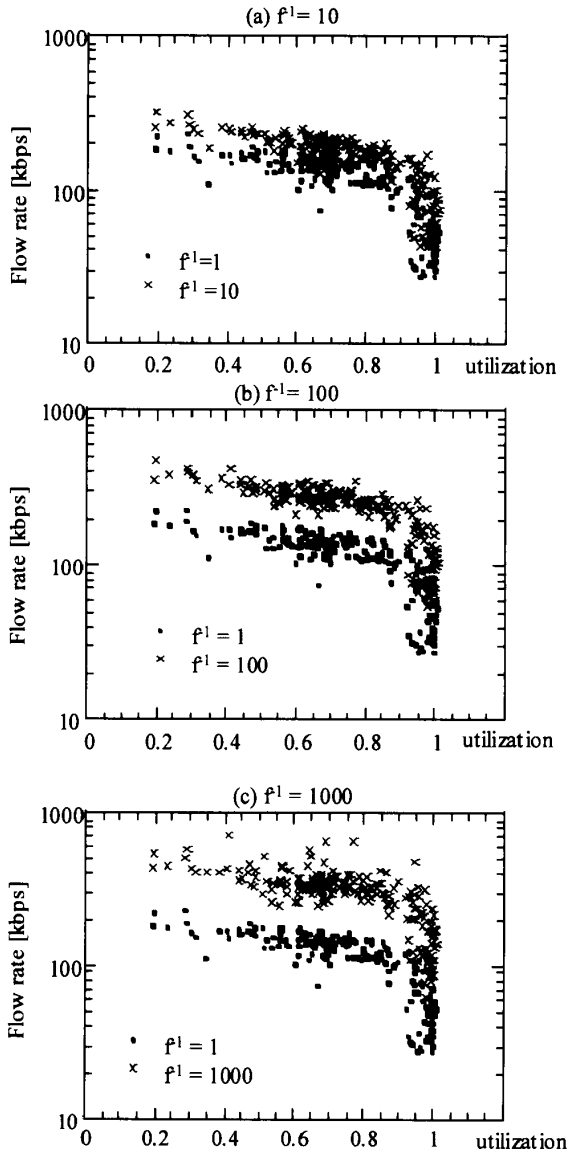

図6 fを変えたときのフローレートvs使用率

[1] 節3.1で，サンプルされたフローレートの方が元のそれよりも高レートとなるために先に劣化すると述べたが，ここでの両者の劣化の様子はほぼ同様にみえる．これは，$f^{-1}=1$のときのF_{avg}が149 kbpsなのに対し，$f^{-1}=1,000$の場合は374 kbpsであり，それらの差が集約リンク帯域17 Mbpsからみてわずかであることに起因する[3]．

グしない場合(i.e., $f^{-1}=1$)に各測定時点において品質劣化が起きているかどうかを節3.2の手順に従って判定し，それを真の品質劣化とみなした．そのように定義される真の品質劣化に対して，$f^{-1}=10, 100, 1000$でサンプリングした場合に誤って品質劣化と判定した割合，および品質劣化を見逃した割合を評価した．

まず，節3.2のStep 2におけるF_{avg}（リンク非輻輳時のフローレート）を計算した（表2）．ここでのF_{avg}は，全測定データ（195個）のうち，$\rho_0(=0.6)$未満のときのフローレートを抽出して計算した．このF_{avg}を用いて，Step 3に従って各測定データが品質劣化状態にあるか否かを判定した．その結果を表3に示す．ここでは，誤って品質劣化と判定する割合FPR，および品質劣化を見逃す割合FNRを評価した．FPRおよびFNRは，次で定義される．

$$\mathrm{FPR}=\frac{N_{FP}}{N_{FP}+N_{TN}}=\frac{N_{FP}}{N_{ndgr}} \tag{7}$$

$$\mathrm{FNR}=\frac{N_{FN}}{N_{FN}+N_{TP}}=\frac{N_{FN}}{N_{dgr}} \tag{8}$$

ここで，N_{FP}は誤って品質劣化と判定された回数，N_{FN}は誤って品質維持（i.e., 品質が劣化していない）と判定された回数，N_{TP}は正しく品質劣化と判定された回数，N_{TN}は正しく品質維持と判定された回数を表す．また，N_{dgr}は真の品質劣化回数（i.e., サンプリング間隔$f^{-1}=1$のときの品質劣化検出回数），N_{ndgr}は真の品質維持回数を表し，$N_{dgr}=64$, $N_{ndgr}=131$であった．表3に，サンプリング間隔を変えたときのFPRおよびFNRを示す．これより，いずれの割合も小さく抑えられていることが確認できる．

参考として，サンプリング間隔f^{-1}を変えたときのサンプルされるフロー数の割合を図7に示す．これより，例えば$f^{-1}=1,000$にすれば，管理すべきフロー数を1/100に削減できることが分かる．

表2 リンク非輻輳時のフローレートF_{avg}[kbps]

f^{-1}	1	10	100	1000
F_{avg}	149	210	300	374

表3 品質劣化検出精度評価

f^{-1}	FPR	FNR
10	0.0076	0.031
100	0.023	0.078
1000	0.038	0.094

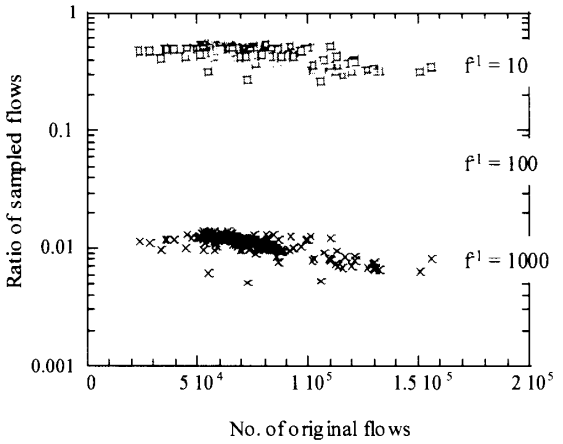

図7 サンプルされるフロー数の割合vs元のフロー数

4. 関連研究

サンプルパケットからフロー統計情報を推定する方法に関する検討がいくつか報告されている．文献[6]はサイズの大きなフローの統計を精度良く得ることを目的としており，本稿で紹介したエレファントフロー特定手法が目指す目的と最も近い．文献[6]の方法では，パケットサンプリングでサンプルされたフローのみの情報を管理すればよいので，フロー管理のためのメモリ量を節約することが可能である．しかし，到着するすべてのパケットに対して，そのパケットがフロー管理メモリ上にエントリされているかどうかチェックし，エントリされていれば管理情報を更新する処理が必要となる．これに対し，本稿で紹介したエレファントフロー特定手法では，パケット毎の処理を必要とせず，サンプルパケットのみを用いているため，必要なメモリ量およびパケット処理量とも削減可能である．

文献[7, 8]では，サンプルされたTCP-SYNフラグの数を用いて，元のフロー発生数やフローサイズに関する統計情報を推定する方法を提案している．また，文献[9]は，複数のhash関数の組み合わせから成るSCBF（Space Code Bloom Filter）を複数個用意し，それらに異なるサンプリングレートでパケットを挿入することにより，サイズ分布の裾野が重い場合にも対応して，フローごとのサイズを少ないメモリ量で把握することを可能にする手法を提案・評価している．しかしいずれの文献[7~9]も，元のフローサイズを推定する手法であり，あるリンク上でのフロー品質劣化検出を可能にするものではなかった．

5. おわりに

本稿では，サンプルパケット情報からトラヒック制御・品質管理に有用な統計情報を推定する手法につい

て，著者らのこれまでの検討結果を二つ紹介した．まず，回線帯域の占有率が大きいユーザフロー（エレファントフロー）を特定する手法について説明した．これは，パケットサンプリングによってサイズの大きいフローがサンプルされる確率が高いことを利用している．サンプルされたパケット数があらかじめ定めたしきい値を超えたらエレファントフローであると判定する方法を提案し，そのしきい値を理論的に導出し，実データを用いて検出精度の評価を行った．また，サンプルパケット情報からTCPフローレベルの品質劣化を検出する方法についても説明した．提案手法では，すべてのフローを管理することなく，フロー全体の中で輻輳に敏感な高レートフローの挙動をパケットサンプリングで把握することにより，TCPフローレベルの品質劣化検出を可能とする．今後は，提案方法における測定周期やサンプリング間隔の設定方法を確立する必要がある．また，これら提案方法で輻輳による品質劣化を検出し，その輻輳主要因であるユーザフローを特定した後に，どのようにユーザフローを制御していくべきかについても検討していく予定である．

参考文献

[1] IETF Packet Sampling (psamp) Working Group, http://www.ietf.org/html.charters/psamp-charter.html

[2] T. Mori, M. Uchida, R. Kawahara, J. Pan, and S. Goto: "Identifying Elephant Flows Through Periodically Sampled Packets," ACM SIGCOMM Internet Measurement Conference (IMC 2004), Oct. 2004.

[3] 川原, 石橋, 森, 阿部: "サンプルパケット情報を用いたTCPフローレベル性能劣化検出法," 信学技報 TM 2004-34, 2004-07.

[4] K. C. Lan and J. Heidemann: "On the Correlation of Internet Flow Characteristics," Technical Report ISI-TR-574, USC/Information Sciences Institute, July, 2003.

[5] Zhang, et al.: "On the Characteristics and Origins of Internet Flow Rates," ACM SIGCOMM, 2002.

[6] C. Estan and G. Varghese: "New Directions in Traffic Measurement and Accounting," In Proceedings of ACM SIGCOMM, August, 2002.

[7] N. Duffield, C. Lund, and M. Thorup: "Properties and Prediction of Flow Statistics from Sampled Packet Streams," ACM SIGCOMM Internet Measurement Workshop, Marseille, France, November, 2002.

[8] N. Duffield, C. Lund, and M. Thorup: "Estimating Flow Distributions from Sampled Flow Statistics," In Proceedings of ACM SIGCOMM, August, 2003.

[9] A. Kumar, J. Xu, J. Wang, O. Spatschek, and L. Li: "Space-Code Bloom Filter for Efficient Per-Flow Traffic Measurement," In proceedings of IEEE INFOCOM, Hong Kong, China, March, 2004.