

ネットワークを流れるバーストパケットの特定方式と トラヒック特性評価

鈴木 秀章[†] 大坐 畠 智[‡] 萩原 洋一[‡] 寺田 松昭[‡] 川島 幸之助[‡]

[†] [‡] 東京農工大学 〒184-0012 東京都小金井市中町 2-24-16

E-mail: [†] s010032@cs.tuat.ac.jp, [‡] {ohzahata, hagi, m-terā, k-kawa}@cc.tuat.ac.jp

あらまし これまでバーストパケットの解析は TCP 輻輳制御によって起きるバーストを特定することにより、行われてきた。そのため、必ずしも実際の物理層で送られるバーストを特定しているわけではなかった。本論文では、IP ヘッダの識別子(IPID)を用いて、送信側から連続的に送られるパケットを特定する方法を提案し、バーストパケットの解析を行う。この方法により、パケット群から直接、バーストを特定でき、実際にバーストがどのようにネットワークを流れているか解析できる。提案するバーストパケット特定方式を用いて、フロー、ホスト、サブネット、スタブネットの 4 つの単位でバーストを特定し、解析を行った。解析の結果、サブネットやスタブネットのバーストは複数のフローにより、フローベースのバーストと変わらない継続時間で大きなバーストが形成されていることが分かった。また、複数のフローで形成されるバーストは一つのフローで形成されるバーストに比べ、ロス率が大きく、ネットワークに大きな影響を与えている。

キーワード IPID, トラヒック測定, バーストパケット

IP Network Level Burst Packets Identification Methods and Traffic Characteristics Evaluation

Hideaki SUZUKI[†] Satoshi OHZAHATA[‡] Yoichi HAGIWARA[‡] Matsuaki TERADA[‡]
and Konosuke KAWASHIMA[‡]

[†] [‡] Tokyo University of Agriculture and Technology Nakamachi 2-24-16, Koganei City, Tokyo,
184-0012 Japan

E-mail: [†] s010032@cs.tuat.ac.jp, [‡] {ohzahata, hagi, m-tera, k-kawa}@cc.tuat.ac.jp

Abstract Many studies of burst packets analysis have been done by identifying burst traffic which is produced by TCP congestion control. Then, these methods do not identify a burst which is sent back-to-back to IP network. In this paper, we propose a burst identification method which identifies back-to-back packets by sender with identifier of the IP header (IPID). Our proposed method can directly identify the back-to-back packets by a sequential IPID, and analyze how these burst packets are transferred in the IP network. In our evaluations, we analyzed four kinds of burst: flow, host, subnet, and stubnet. These results show that a large size burst of subnet and stubnet is composed of many flows, and their flow duration time are the same as flow based burst. A burst which is composed of many flows is higher loss ratio than the burst which composed of one flow. These bursts give large impact for the network traffic.

1. はじめに

これまでバーストパケットの解析は、TCP 輻輳制御を解析することにより、行われてきた[1]。これは、輻輳ウィンドウサイズやパケットロスなどからバーストを、特定し解析が行われることとなる。具体的には、パケットロスが発生した際の高速リカバリにより、輻輳ウィンドウサイズの半分のパケットが送られる部分や、ACK パケットがロスした際、バーストを促す部分

などがあり、これらを特定することでバーストパケットを特定してきた。他にも、パケットが送信される時間間隔によって特定する方法[2]や送信が成功した ACK パケットにより、その間に送られたパケットを特定する方法[3]などが挙げられる。

本論文では、IP ヘッダの ID フィールド (IPID) に振られる連続値を用いて、送信ホストが連続で送るバーストパケットを特定する。これにより、実際にネットワーク上をどのようにパケットが流れ、バーストが

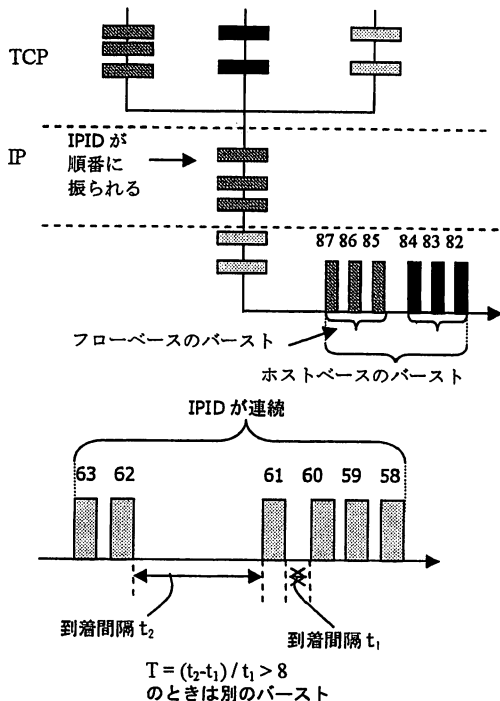


図1 フロー、ホストにおけるバースト。

パケットロスにどのような影響を与えているかを明らかにする。

2. バーストパケットの特定方法

これまでの TCP 層でのバーストパケットの特定方法は TCP 層で生成されるバーストを特定して解析を行ってきた。これは、ホストによっては実際の物理層でのバーストとは異なる場合も出てくる。そこで、本論文では IP 層で振られる IPID を用いて、実際の物理層で送られるバーストを特定する方法を提案する。

バーストパケットをフロー、バースト、サブネット、スタブネットごとに IPID を用いて特定する。IPID とは送信側のホストにおいて、パケットを送信するたびに連続的に振られる値のことである。IP ヘッダの ID フィールドに格納され、この値を利用することで、送信元から実際に連続的に IP ネットワークに送られるパケットを特定することが可能となる。

2.1 フロー、ホストベースのバースト

まず、フローベースのバーストパケットの特定方法について図1に示す。ここで、フローとは送受信 IP アドレス、送受信ポート番号、プロトコルの5つのユニークな組み合わせで定義される。図1では1つのホストにおいて、複数のコネクションが張られている場合、どのように IPID が振られているかを示している。OS では TCP 層から IP 層にパケットを送る際にスケジューリングが行われ、その際、IP 層で IPID が順番に振られることになる。よって、IPID が連続している部分を特定することで、実際に物理層で送られるバースト

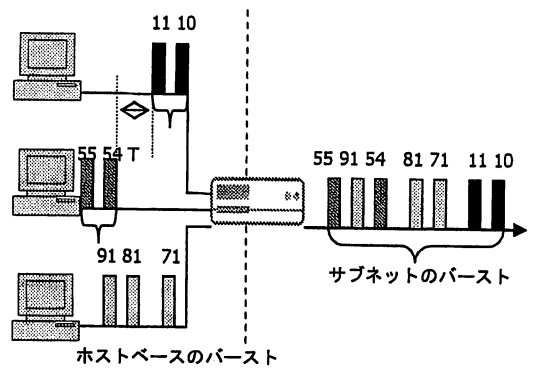


図2 サブネット、スタブネットにおけるバースト。

を特定することが可能となる。

しかし、送信側のホストが複数のコネクションを確立していない場合、IPID は連続で送られている部分以外でも連続的に振られてしまう。この場合、バーストパケット群を見つけることができなくなってしまう。このような場合は、参考文献[2]を基にパケット到着間隔を考慮する。ここで、パケット到着間隔を比べる際、図1の式において、よく用いられる2, 4, 8の値から最大値の8を用いて特定を行った。

ホストベースのバーストの特定方法は同様に図1に示す。ホストベースのバーストは送信側のホストにおいて連続して IPID が振られている部分をバーストとする方法である。ホストは送信側の IP アドレスによって特定する。

2.2 サブネット、スタブネットベースのバースト

次に、サブネット、スタブネットにおけるバーストの特定方法を図2に示す。図2ではルータに複数のホストからバーストパケットが送られてくる様子を示している。2.1で示したフローベース、ホストベースのバーストパケットの特定方法により特定したバーストがルータで送られるとき、図2のようにバーストの間隔が“T”で送られる場合がある。この“T”が前のパケットの間隔の8倍以内であれば、同じバーストとして扱うこととする。また、ローカル IPID(各フローで1つのカウンタを持つ IPID)を持ったフローが図2のように、特定したサブネットのバーストに含まれる場合、これらも加えることとする。これを繰り返すことでサブネット、スタブネットベースのバーストを求めることにする。なおサブネットベースのバーストは****.***.0/24 単位の IP アドレスでまとめたバーストであり、スタブネットのバーストは****.***.***.0/16 単位の IP アドレスでまとめたバーストのことを指す。スタブネットのバーストは同じクラスBのネットワークアドレスであり、サブネットのバーストをまとめたものである。

3. トラフィック測定

評価に用いたデータを表1に示す。まず、農工大キャンパスネットワークにおいて、上流の SINET 東京農工大学ルータと下流の東京農工大学ルータ間を流れるデータの IP, TCP ヘッダ部分を測定したものをを用いる。

表1 トラフィック測定場所.

測定機関	測定日時	リンク
農工大	2005/1/20, 12:00-16:00	100Mbps
WIDE	2005/9/22, 14:00-15:00	trans-Pacific line 100Mbps
NLANR	2002/08/14, 9:00-10:00	OC-48(2.4Gbps)
CAIDA	2003/04/24, 0:00-1:00	OC-48(2.4Gbps)

また、農工大ネットワークは混んでいることが比較的少ないので、比較対象として、ネットワークが混んでいる WIDE プロジェクト [4], NLANR [5], CAIDA [6] のログを利用している。測定日時やリンクは表 1 のようになっている。

4. 解析結果

4.1 ネットワークの状況

はじめに各機関のネットワークの状況がどのようになっているかを調べる。まず、平均利用帯域とロス率を算出する。これで、各機関のネットワークがどのような特徴があるのかを調べる。

表2 各機関の利用帯域とロス率.

測定機関	平均利用帯域(Mbps)	ロス率(%)
農工大	13.6	1.49
WIDE	25.1	5.68
NLANR	134.3	0.83
CAIDA	65.1	6.33

表 2 より、農工大、NLANR は比較的ロス率が低いため、あまり混んでいないことが分かる。一方で、WIDE、CAIDA はロス率が高いことが分かる。この輻輳状態の違いに着目して解析を行う。

4.2 パーストの統計

次に、特定したパーストの統計を示す。各機関でフロー、ホスト、サブネット、スタブネットごとに求めたパーストサイズの補分布を図 3-6 に、パースト継続時間の補分布を図 7-図 10 に示す。図ではフローベースのパーストを“Flow”，ホストベースのパーストを“Host”，サブネットベースで求めたパーストを“Subnet”，スタブネットベースで求めたパーストを“Stubnet”で示している。

図 3-図 6 より、フローベースのパーストは 64KB 付近で大きく下がっていることが分かる。これは、TCP 輻輳制御における最大のウィンドウサイズがデフォルトで 64KB であることから、フローベースのパーストではこれ以上大きなパーストが作られることはほとんどないためであると考えられる。ただし、TCP オプションなどにより、64KB 以上のパーストが作られることもある。ログではこの TCP オプションも観測されており、フローベースのパーストがすべて 64KB で収まっているわけではない。よって、本論文で提案する解析方法が正しくパーストを推測できていることが分かる。

次にホストベースのパーストを見ると、フローベースのパーストとサイズはあまり変わっていないことが

分かる。これは測定地点においてホストベースのパーストが通過しなかったためである。1 つのホストにおいて連続して送信されたパーストが、必ずしも測定地点までそのまま送られるわけではなく、測定地点の手前で別の場所に送られるフローもあるためであると考えられる。よって、ホストベースのパーストは測定地点に依存しており、送信側に近い場所で測定すると、フローベースのパーストとホストベースのパーストの違いが見られ、受信側に近い場所で測定するとほとんど違いが見られないものと考えられる。

サブネット、スタブネットベースでは、パーストサイズは最も大きいもので 100MB 近くあることが分かる。これは、フローおよびホストベースのパーストの 100 倍近い大きさである。

一方、パーストの継続時間は、フロー、ホスト、サブネット、スタブネットできほど大きな差が見られない。つまり、ホストベースのパーストに他の小さなホストベースのパーストが重なり、100MB 近い大きなパーストが形成されていることが分かる。

ここでこれらのパーストはどの程度のフロー数で構成されているかをパーストサイズ別に平均を算出して求めた。これを図 11-図 14 に示す。

図より、サブネット、スタブネットのパーストはかなり多くのフローから構成されていることが分かる。特に、NLANR、CAIDA では 60KB を超えたあたりから大きくなっている。一方で農工大ではほとんど変化がない。これは測定場所が受信側に近いためである。

よって、複数のフローにより、フローベースのパーストと変わらない継続時間で大きなパーストが形成されていることが分かる。

4.3 パーストサイズとロス率

次に、フロー、ホスト、サブネット、スタブネットそれぞれで求めたパーストについて、パーストサイズ別にパーストロス率を求めた。ここで、パーストロス率は以下の式で求められる。

$$\text{パーストロス率} = \frac{\text{ロスがあったパースト数}}{\text{全体のパースト数}}$$

これは 1 つのパーストにおいて、1 つでもパケットロスが発生しているパーストの割合を算出したものである。TCP 輻輳制御では 1 つでもパケットロスが生じれば、ウィンドウサイズが半分になり、通信効率が低下するため、このような算出方法で求める。これを図 15-図 18 に示す。

図 15-図 18 より、どの機関でもフローベースとホストベースのパーストロス率はさほど大きな差はないが、サブネット、スタブネットベースの順でパーストロス率が大きくなっていることが分かる。また、パーストサイズが大きくなるにつれて、フロー、ホストベースのパーストに比べ、その差が大きくなっている。フローベースのパーストは TCP 輻輳制御により、ネットワークの輻輳状態を考慮して、徐々にウィンドウサイズが大きくなって作られたパーストである。よって、大きなパーストであっても、それほど大きなロス率になっていない。一方、サブネットやスタブネットベースのパーストは、複数のフローベースのパーストにより構成されている。よって、各々のフローにおいて TCP

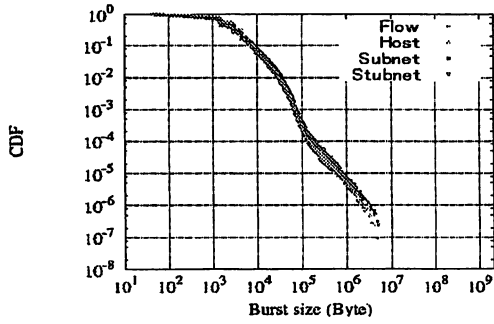


図3 バーストサイズの補分布(農工大).

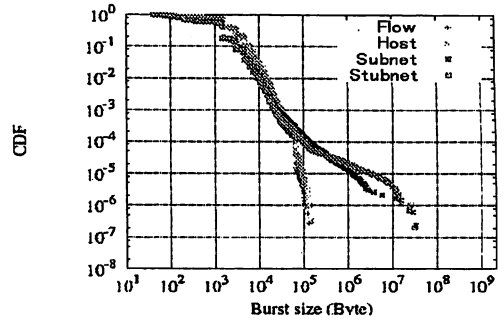


図4 バーストサイズの補分布(WIDE).

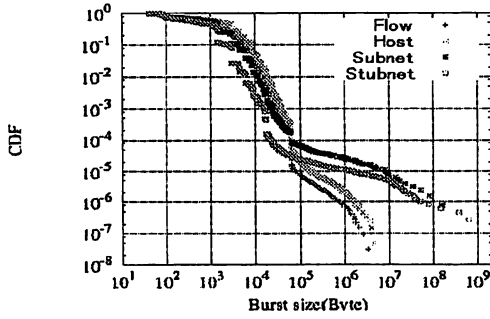


図5 バーストサイズの補分布(NLANR).

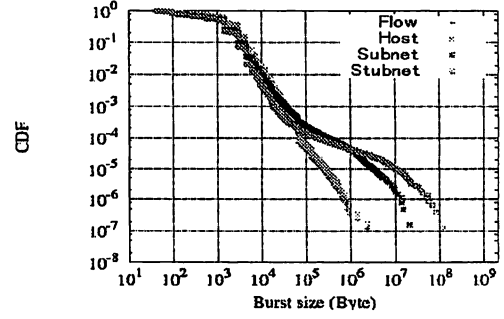


図6 バーストサイズの補分布(CAIDA).

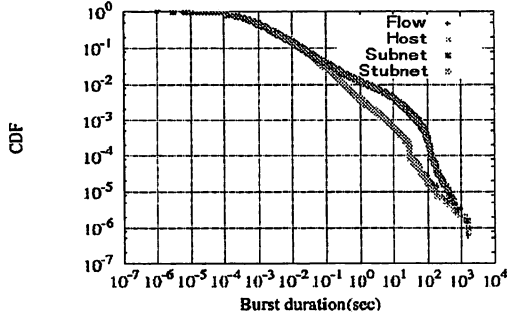


図7 バースト継続時間の補分布(農工大).

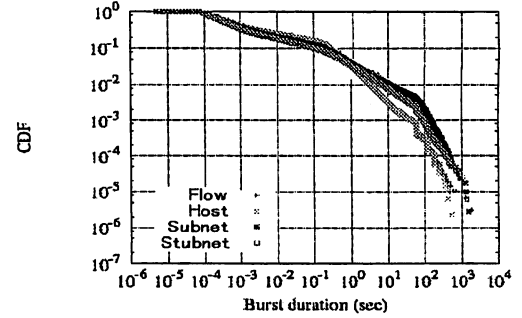


図8 バースト継続時間の補分布(WIDE).

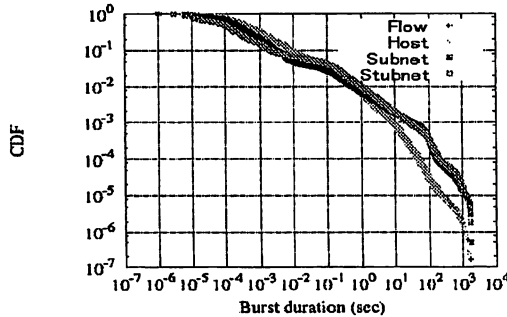


図9 バースト継続時間の補分布(NLANR).

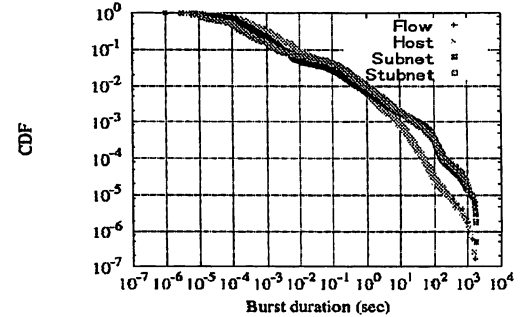


図10 バースト継続時間の補分布(CAIDA).

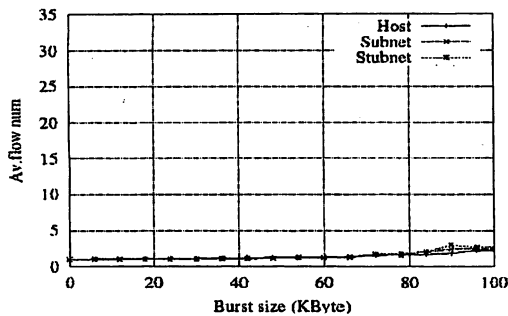


図 11 パーストサイズ別平均フロー数 (農工大).

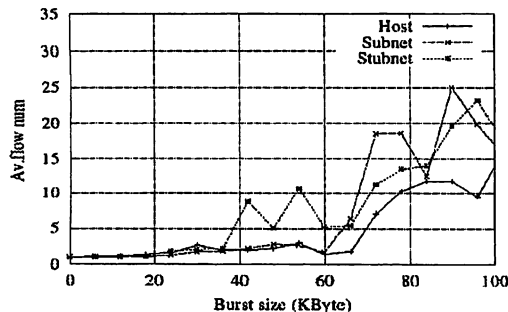


図 13 パーストサイズ別平均フロー数 (NLANR).

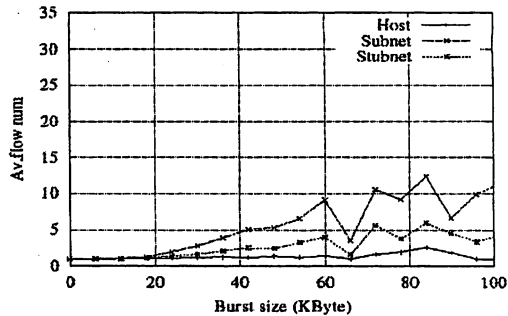


図 12 パーストサイズ別平均フロー数 (WIDE).

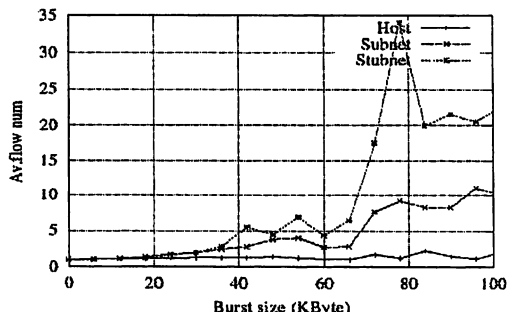


図 14 パーストサイズ別平均フロー数 (CAIDA).

輻輳制御が行われていても、複数のフローが重なって大きなバーストを形成した場合、TCP 輻輳制御では制御できずにロスが発生している。よって、フローベースのバーストに比べ、大きなバーストになるほど、バーストロス率が高くなっていることが分かる。

つまり、フローベースのバーストはそれほどネットワークに大きな影響を与えていないが、複数のフローが重なって形成されるバーストはネットワークに大きな影響を与えていると考えられる。農工大においては、サブネットのバーストがほとんどフローベースのバーストと一致しているため、大きな差が見られない。

4.4 1つのフローと複数のフローからなるバーストの比較

ホスト、サブネット、スタブネットではバーストが1つのフローで形成される場合と複数のフローで形成される場合がある。この2種類のバーストではバーストロス率にどのような差が見られるかを解析する。解析結果を図 19-図 22 に示す。なお、図において、1つのフローで形成されるバーストを“One flow”で示し、複数のフローで形成されるバーストを“Many flows”で示している。

図 19-図 22 より、1つのフローで形成されるバーストに比べ、複数のフローで形成されるバーストはロス率が高くなっていることが分かる。これは、1つのフローで形成されるバーストは TCP 輻輳制御が働いているため、ロスの発生が抑えられている。一方、複数のフローで形成されるバーストは、ルータの部分で複数のフローのバーストが重なり合い、輻輳を起こすことにより、ロスが発生していることが考えられる。

すなわち、ネットワークにおいてロスが発生するのは、複数のフローのバーストがルータ部分で重なり合うことにより発生していることが分かる。つまり、各々の TCP フローで制御が行われていても、大きなバーストが来たとき、そのバーストに巻き込まれてロスとなる可能性があることが分かる。

5. おわりに

本論文では連続して(back-to-backで)送られるパケットに注目してバーストパケットの特定方法の提案を行い、バーストパケットの解析を行った。その結果、サブネット、スタブネットベースで特定したバーストはロス発生に大きな影響を与えていることが分かった。今後の課題として、TCP 輻輳制御で制御できないパケットロスに対して、どのような制御が必要であるかなどを検討していくことが考えられる。

文 献

- [1] Hao Jiang and Constantinos Dovrolis, “Source-Level IP Packet Bursts: Causes and Effects,” Proc. of ACM SIGCOMM Conference on Internet measurement, pp.301-306, 2003.
- [2] Srinivas Shakkottai, Nevil Brownlee, and kc claffy, “A Study of Burstiness in TCP Flows,” Proc. of PAM 2005, LNCS 2431 pp.12-26, 2005.
- [3] Ethan Blanton and Mark Allman, “On the Impact of Bursting on TCP Performance,” Proc. of PAM 2005, LNCS 3431, pp.1-12, 2005.
- [4] WIDE project, <http://www.wide.ad.jp/>.
- [5] CAIDA, <http://www.caida.org/>.
- [6] NLANR, <http://www.nlanr.net/>.

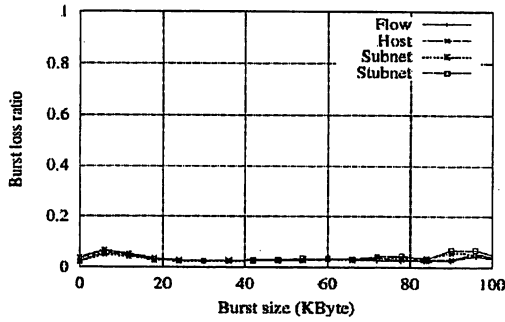


図 15 パーストロス率(農工大).

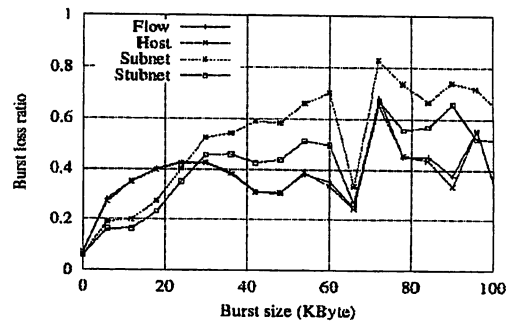


図 16 パーストロス率(WIDE).

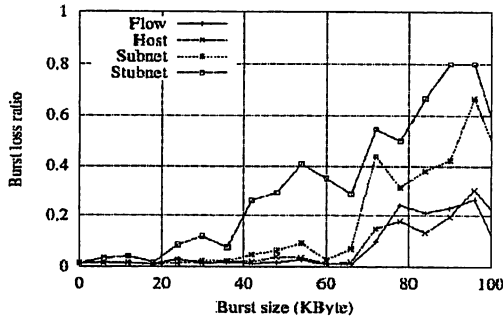


図 17 パーストロス率(NLANR).

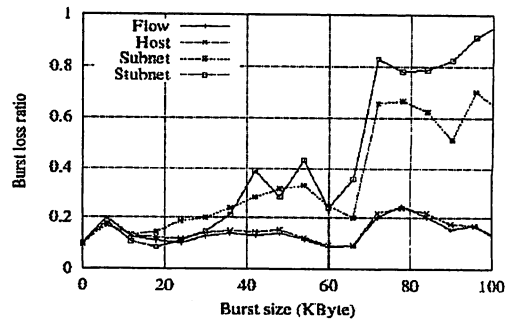


図 18 パーストロス率(CAIDA).

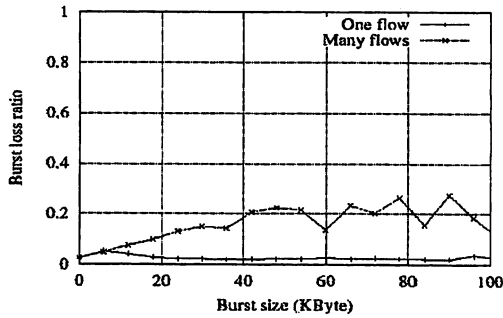


図 19 サブネットフロー数別パーストロス率(農工大).

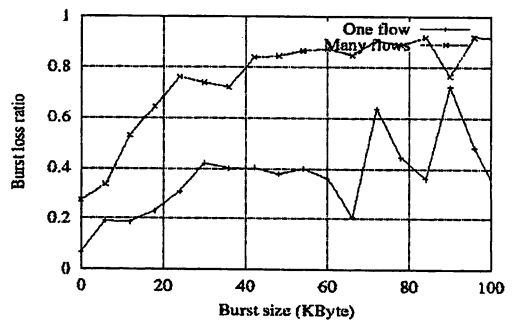


図 20 サブネットフロー数別パーストロス率(WIDE).

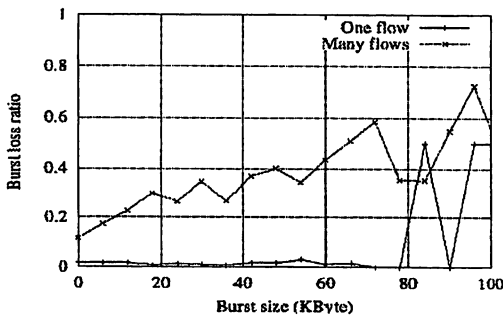


図 21 サブネットフロー数別パーストロス率(NLANR).

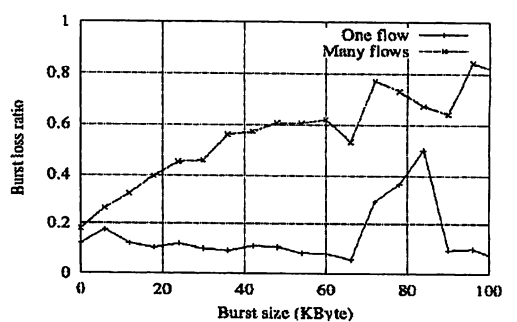


図 22 サブネットフロー数別パーストロス率(CAIDA).