# 基于最小二乘法的流长度分布估计方法

刘卫江[1,2,3] 龚 俭[2,3] 丁 伟[2,3] 程 光[2,3]

([1] 东南大学计算机科学与技术学科博士后流动站, 南京 210096)
([2] 东南大学计算机科学与工程学院, 南京 210096)
([3] 江苏省计算机网络技术重点实验室, 南京 210096)

**摘要**: 为了得到未抽样流的分布特征, 提出一种新的由抽样报文流数据来估计原始未抽样流长度分布的方法. 首先分析了产生一个定长抽样流的原始流的概率分布模型, 并根据这个概率分布特征给出了长流一个非常简单的估计. 然后构造了关于短流的方程组, 利用流的重尾分布特性和最小二乘法对该方程组进行求解, 得到了短流的估计. 理论分析表明该估计方法有效地控制了时间复杂程度, 实验测试结果也表明该算法对于分布的估计是精确的, 估计精度与 EM 算法相当.

**关键词**: 抽样报文; IP 流; 概率; 最小二乘法

**中图分类号**: TP393 **文献标识码**: A **文章编号**: 1001 - 0505(2006)03-0467-05

# Method for estimation of flow length distributions based on least square method

Liu Weijiang[1,2,3] Gong Jian[2,3] Ding Wei[2,3] Cheng Guang[2,3]

([1] Post Doctoral Station for Computer Science and Technology, Southeast University, Nanjing 210096, China)
([2] School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)
([3] Key Laboratory of Computer Networking Technology of Jiangsu Province, Nanjing 210096, China)

**Abstract**: A novel method for estimation of original flow length distributions from sampled flow statistics is proposed to obtain the distribution feature of unsampled flows. First, the probability distribution model of original flow for a sampled flow of fixed length is analyzed, and simple estimation for large flows is described according to the analysis result. Then, estimation for short flows is obtained by constructing equations involving short flows and solving them using the heavy-tailed feature of flow and the least square method. The theoretical analysis shows that the computational complexity of this method is well under control, and the experimental results demonstrate that the distributions inferred from the proposed method are as accurate as those from the expectation maximum (EM) algorithm.

**Key words**: packet sampling; IP flows; probability; least square method

网络流量测量是网络管理的需求[1], 短期的流量测量可用于网络运行管理, 如监测网络热点、防止 DoS 攻击、流量计费等; 长期的流量测量可用于流量工程和网络规划. 在被动测量中, 越来越多的测量系统对报文进行抽样采集来减少对系统资源的消耗, 许多高端路由器也是通过使用报文的抽样子流来形成流统计数据的, 以减少在流查找过程中存储和处理的数据量. 早在 1993 年 Claffy 等[2]就系统研究了以时间和报文到达次序为激发机制的抽样, 分析了系统抽样、随机抽样分层的测量技术. 进入 21 世纪以后, 由于 2.5 Gbit/s 和 10 Gbit/s 高速主干网络的普遍使用和网络流量测量的广泛应用, 抽样测量技术有了较快发展. 2003 年 IETF 成立了报文抽样测量工作组(PSAMP)[3], 专门用于研究报文抽样测量技术. 美国 AT&T 实验室的 Duffield 等于 2001 年提出了 Trajectory 基于报文内容的抽样技术[4], 后来又在文献[5]中研究了

**收稿日期**: 2005-11-30.
**基金项目**: 国家重点基础研究发展计划(973 计划)资助项目(2003CB314803)、教育部科学技术研究重点资助项目(105084)、江苏省网络与信息安全重点实验室资助项目(BM2003201)、江苏省博士后科研资助计划资助项目.
**作者简介**: 刘卫江(1969—), 男, 博士, 教授, wjliu@njnet.edu.cn.

Trajectory 抽样的应用. 同时抽样测量技术也开始应用于网络产品中,如 Cisco 的 Netflow[6] 和 NetranMet 测量器[7].

抽样会造成一些内在信息的损失,因此可使用推断估计的方法来减少这种损失. 目前从抽样报文统计数据来推断出原始的未抽样流的流分布特征的研究主要集中在部分流和全部流长度分布这 2 个方面. 2003 年 Estan 等提出了 2 种算法用于发现长流:抽样保持(sample and hold)和多级过滤(multistage filters),有效地解决了如何在报文抽样情况下获取和维护流信息的问题[8]. Hohn 等在理论上对报文抽样和流抽样 2 种抽样方法进行了比较,指出由报文抽样进行估计在抽样比率达到 0.01 或更小时在估计精度方面的局限性[9]. 尽管报文抽样方法在网络测量中已经被广泛使用,但由报文抽样流估计原始流分布的研究工作还是较少. Duffield 等首先在这方面进行了研究,提出由抽样流数据推断出原始流数据的思想,特别是对平均流长度的推断[10],并提出了 2 种推断方法:比例法(scaling method)和 EM 算法[11]. 比例法算法简单,由抽样数据很容易就可以计算出原始的未抽样的统计数据,但这种方法只能用于对 TCP 流的抽样估计,抽样时要对 SYN 报文进行统计,对于没有 SYN 报文的 UDP 流不适用. EM 算法既适用于 TCP 流也适用于普通流,缺点是计算量太大.

本文给出一种新的由抽样报文统计数据来推断原始报文流分布的方法,此方法不仅适用于 TCP 流,对于普通流也是可行的. 首先把流按被抽空(一个报文也不被抽到)概率的不同分为长流和短流. 对于长流给出了一个非常简单易算的估计方法,认为它是由可产生它的最大概率的几个原始流产生的. 对于短流构建了一个方程组,对该方程组利用流的重尾特性和最小二乘法进行求解,得到了对于短流的估计.

## 1 抽样估计的基本概念

本文考虑从报文序列中抽样出 $p=1/N$ 部分,在概率抽样中可以有多种方法进行抽样:一种是通过产生一个随机数,来确定 $N$ 个报文中抽哪一个,另一种是定期抽样,每 $N$ 个报文抽取第 $N$ 个. 这 2 种方法在文献[11]中已经进行了比较,显示了 2 种方法得到的结果是足够相近的. 由于研究的背景不同,对于流采用了不同的定义. 本文采用文献[12]中的定义.

**定义 1** 流是指符合特定的流规范和超时约束的一系列报文的集合. 本文中 TCP 流是指具有相同的源 IP、宿 IP、源端口、宿端口的在超时约束下的 TCP 报文集合,普通流是指具有相同的源 IP、宿 IP、源端口、宿端口的在超时约束下的 TCP 或 UDP 报文集合(不考虑协议).

**定义 2** 抽样流是指在上述定义的流中以概率 $p=1/N$ 进行概率抽样而得到的报文集合.

**定义 3** 超时是指一个流中相邻报文的最大时间间隔,它决定什么时候结束一个流.

**定义 4** 流长度是指一个流中所包含的报文的数量. 例如对一个含有 10 个报文的流,则这个流的长度为 10.

本文为叙述方便称定义 1 中的流为原始流,本文的目的是给出由一个抽样流的分布而推断出它所对应的原始流分布的方法.

## 2 原始流长度的分布模型

本文中所有的抽样都是以 $p=1/N$ 为概率的. 对于一个固定的原始流 $F$,令 $X_F$ 为 $F$ 的原始报文数量,$Y_F$ 为 $F$ 的抽样流的报文数量. 给定 $X_F=l$,则 $Y_F=k$ 的概率 $P[Y_F=k|X_F=l]$ 是二项分布,为 $B_p(l,k)=\binom{l}{k}p^k(1-p)^{l-k}$. 对于一个原始流 $F$,$P[Y_F=y, X_F=x]$ 表示 $X_F=x, Y_F=y$ 的概率,根据条件概率公式,有

$$P[X_F=x|Y_F=y]=\frac{P[Y_F=y,X_F=x]}{P[Y_F=y]}=\frac{P[Y_F=y|X_F=x]P[X_F=x]}{P[Y_F=y]}$$

根据全概率公式有

$$P[Y_F=y]=\sum_{i=y}^{\infty}P[Y_F=y|X_F=i]P[X_F=i]=\sum_{i=y}^{\infty}B_p(i,y)P[X_F=i]\qquad y=0,1,\cdots$$

把均匀分布作为原始流长度的先验分布,则有 $P[X_F=k]=P[X_F=k+1], k=1,2,\cdots$. 而

$$\sum_{l=k}^{\infty}B_p(l,k)=\sum_{l=k}^{\infty}\binom{l}{k}p^k(1-p)^{l-k}=p^k\sum_{l=0}^{\infty}\binom{l+k}{k}(1-p)^l=p^k\sum_{l=0}^{\infty}\binom{l+k}{k}q^l=p^k(1-q)^{-k-1}=\frac{1}{p}=N$$

于是有 $P[Y_F=y]=\sum_{i=y}^{\infty}B_p(i,y)P[X_F=i]=P[X_F=y]\sum_{i=y}^{\infty}B_p(i,y)=\frac{P[X_F=y]}{p}$,故有

$P[X_F=x\mid Y_F=y]=$

$$\frac{P[Y_F = y \mid X_F = x]P[X_F = x]}{P[Y_F = y]} = \frac{P[Y_F = y \mid X_F = x]P[X_F = x]}{P[X_F = y]/p} = pB_p(x,y)$$

因此得到

**引理 1**　一个长度为 $k$ 的抽样流由长度为 $l$ 的原始流抽样产生的概率分布为

$$P[X_F = l \mid Y_F = k] = \binom{l}{k} p^{k+1}(1-p)^{l-k}$$

$$l = k, k+1, \cdots$$

本文为了表达简单,用 $P(l,k)$ 表示 $P[X_F = l \mid Y_F = k]$.

下面计算此概率的数学期望和方差.

**引理 2**　一个长度为 $k$ 的抽样流由长度为 $l$ 的原始流抽样产生的概率分布的数学期望 $E[\xi] = N(k+1) - 1$,方差 $D[\xi] = (N+1)N(k+1)$.

记 $a_1 = \dfrac{P(l,k)}{P(l-1,k)} = \dfrac{(l-1)(1-p)}{l-k-1} = 1 + \dfrac{k-(l-1)p}{l-k-1}$,当 $l < kN+1$ 时,$a_1 > 1$,因此 $P(l,k)$ 随着 $l$ 的增加而递增;当 $l > kN+1$ 时,$a_1 < 1$,因此 $P(l,k)$ 随着 $l$ 的增加而递减. 而当 $l = kN+1$ 时,$a_1 = 1, P(l,k) = P(l-1,k)$ 达到最大值.

**引理 3**　引理 1 中分布的概率值在 $l = kN, kN+1$ 时达到最大,当 $l < kN+1$ 时随着 $l$ 的增加而增加,当 $l > kN+1$ 时随着 $l$ 的增加而减少.

## 3　原始流分布的估计方法

### 3.1　流的分类

记抽样流分布为 $g = \{g_j : j = 1,2,\cdots,n\}$,其中 $g_j$ 表示长度为 $j$ 的抽样流数量,记估计出的原始流分布为 $f = \{f_i : i = 1,2,\cdots,n,\cdots\}$,其中 $f_i$ 表示长度为 $i$ 的原始流数量. 首先计算某个原始流一个报文也没被抽到的概率. 考虑一个长度为 $Nj$ 的原始流,它未被抽到报文的概率为 $(1-1/N)^{Nj} = ((1-1/N)^N)^j$,数列 $\{(1-1/N)^N\}$ 是单调增加的,并且 $\lim\limits_{N\to\infty}(1-1/N)^N = 1/\mathrm{e} < 0.37$,对于可以允许的误差 $\varepsilon$,$(1-1/N)^{Nj} < (1/\mathrm{e})^j < \varepsilon$,只需 $j_{\mathrm{bord}} \geqslant j(\varepsilon) = \mathrm{ceil}(\log(1/\varepsilon))$,例如 $j(0.01) = 5, j(0.001) = 7$. 对于一个固定的阈值 $\varepsilon$,当一个流不被抽到的概率大于这个阈值时,称为短流,否则称为长流. 由于流长度的不同,它们被抽到的概率也不同,一个长流不被抽到的概率很小,而对于一个短流不被抽到的概率较大. 下面分别对长流和短流给出不同的估计算法.

### 3.2　长流的估计

对于一个长度为 $j > j_{\mathrm{bord}}$ 的抽样流,根据引理 3 可知,概率最大的 $2N$ 个原始流的长度整数区间为 $[Nj-N+1, Nj+N]$,估计这个抽样流是由这 $2N$ 个流中某个流抽样而得到的. 记 $\mathrm{sum}(j) = \sum\limits_{l=Nj-N+1}^{Nj+N} P(l,j)$,则 $g_j$ 个抽样流中有 $\dfrac{P(l,j)}{\mathrm{sum}(j)} g_j$ 个是长度为 $l$ 的原始流抽样得到的,于是对 $i > Nj_{\mathrm{bord}}$ 有

$$f_i = \frac{P(l,j)}{\mathrm{sum}(j)} g_j + \frac{P(l,j+1)}{\mathrm{sum}(j+1)} g_{j+1}$$

式中

$$j = \left\lfloor \frac{i-1}{N} \right\rfloor \tag{1}$$

### 3.3　短流的最小二乘法估计

对于 $i \leqslant Nj_{\mathrm{bord}}$ 的原始流可以由下面的方程组估计:

$$g_j = \sum_{i=j}^{m} B_p(i,j) f_i \tag{2}$$

式中,$m = \max\{i : f_i \neq 0\}$,$j = 1,2,\cdots,Nj_{\mathrm{bord}}$,对于 $i > Nj_{\mathrm{bord}}$ 的 $f_i$ 可以用式(1)的结果代入而得到下面的方程组:

$$\bar{g}_j = g_j - \sum_{i=Nj_{\mathrm{bord}}+1}^{m} B_p(i,j) f_i = \sum_{i=j}^{Nj_{\mathrm{bord}}} B_p(i,j) f_i$$

$$j = 1,2,\cdots,Nj_{\mathrm{bord}} \tag{3}$$

对于 $\bar{g}_j$,若其小于或等于 0,则用 $\delta \bar{g}_{i-1}$ 来代替,这里 $0 < \delta < 1$,例如可取 $\delta = 0.94$. 通过上面的处理后可以保证所有的 $\bar{g}_j$ 都大于零. 但由于式(3)中的很多系数可能为零,或很小,而导致结果有很大的偏差. 对 $i \geqslant 8$ 的流利用流的重尾分布特性进行处理,对于 $i, l \in [8, Nj_{\mathrm{bord}})$ 有 $\dfrac{\log f_i - \log f_l}{\log l - \log i} = k$,$k$ 是大于零的实数,进一步变形可得

$$f_i = \left(\frac{l}{i}\right)^k f_l \tag{4}$$

把式(4)代入式(3)得

$$\bar{g}_j = \sum_{i=j}^{l} B_p(i,j) f_i + \sum_{i=l+1}^{Nj_{\mathrm{bord}}} B_p(i,j) \left(\frac{l}{i}\right)^k f_l$$

$$j = 1,2,\cdots,Nj_{\mathrm{bord}} \tag{5}$$

取 $k \in [1.0, 5.0]$,每次增加 0.1,对每一个 $k$ 做如下计算:

把式(5)合并同类项整理得

$$y_j = \sum_{i=1}^{l} x_{ji} f_i \qquad j = 1,2,\cdots,Nj_{\mathrm{bord}} \tag{6}$$

由文献[13]可知最小二乘估计是方差最小的无偏估计,利用最小二乘法估计求式(6)的解,并且计算 $m_k = \sum\limits_{j=1}^{Nj_{\mathrm{bord}}} \left(y_j - \sum\limits_{i=1}^{l} x_{ji} f_i\right)^2$. 在所有的正值解中,找出使得对应的 $m_k$ 值最小的 $k$,把这组解及 $k$ 值代入式(4)可求解出所有的短流的分布值.

## 4 分析与实验

### 4.1 计算复杂度分析

设 $j_{\max}$ 为最大的抽样流长度,则为了计算长流需计算的二项式系数次数为 $O(Nj_{\max})$. 为了得到方程组需要计算的二项式系数次数为 $O(NNj_{\text{bord}}j_{\max})$. 为计算最小二乘法而提供的二项式系数次数表为 $O((Nj_{\text{bord}})^2)$,而完成一次最小二乘法计算所需的时间很少. 与目前已知最好的由报文抽样流进行估计的方法——文献[11]中的EM算法进行比较,在文献[11]中完成一次EM迭代为 $O(i_{\max}j_{\text{size}})$,完成一次全部迭代为 $O(i^2_{\max}j_{\text{size}})$. 在CERNET华东北主干网(1 Gbit/s)以每10个报文抽取一个的抽样比例采集了1 min的报头数据,用本文所提出的算法进行计算,取 $\varepsilon = 0.01$,则 $j_{\text{bord}} = 5$,这时 $NNj_{\text{bord}}j_{\max} = 50^3$. 而利用文献[11]中算法进行计算,此时 $i_{\max} = 2\,000$,$j_{\text{size}} = 200$,则 $i^2_{\max}j_{\text{size}} = 6\,400 \times 50^3$. 后者是前者的6 400倍,而且随着采集数据时间的增加文献[11]中的算法时间复杂度还要增加,而本文对短流的EM算法是与采集时间无关的,只与抽样周期 $N$ 和阈值 $\varepsilon$ 有关.

### 4.2 估计精度分析

本文采用文献[11]中的加权平均相对差异(weighted mean relative difference,WMRD)作为评价的测度. 设 $n_i$ 为长度为 $i$ 的流的数量,$\hat{n}_i$ 为被估计的数量,则WMRD定义如下:

$$D = \frac{\sum_i |n_i - \hat{n}_i|}{\sum_i \frac{n_i + \hat{n}_i}{2}}$$

利用在CERNET华东北主干网上采集的1 d的数据,分别以1,5和10 min为时间粒度,并分别以 $N = 10,30,100$ 为抽样周期进行抽样统计,以本文方法与文献[11]中的EM算法进行估计计算.

表1表明本文所提出的估计方法精度与文献[11]中的EM算法的估计精度相近,有时甚至更好.

**表1 本文方法与EM算法的WMRD**

| 时间/min | 抽样周期 | 本文方法的WMRD | EM算法的WMRD |
|---|---|---|---|
| 1 | 10 | 18 | 29 |
| | 30 | 23 | 29 |
| | 100 | 31 | 34 |
| 5 | 10 | 15 | 18 |
| | 30 | 21 | 19 |
| | 100 | 34 | 38 |
| 10 | 10 | 13 | 15 |
| | 30 | 22 | 23 |
| | 100 | 31 | 35 |

图1是1 min数据的原始流分布、EM算法估计和本文方法估计的比较图,从图中可以看出对短流的估计本文方法更准确.

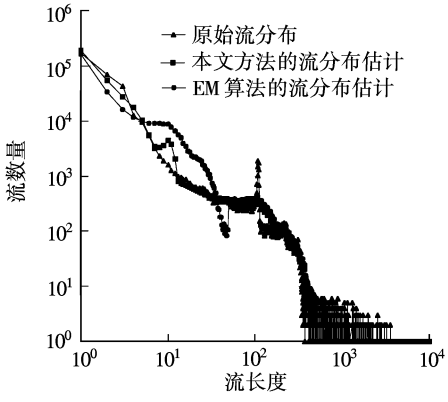


**图1 原始流分布与流分布估计**

按不同的时间粒度和抽样概率进行比较,可以发现 $N = 10,30$ 时的抽样估计是很准确的,但 $N = 100$ 时偏差较大,即当采集报文的时间粒度较长的时候估计的精确度提高了.

## 5 结 语

本文给出了一种新的由抽样报文数据来估计原始流分布的方法,研究了一条抽样流的原始流的分布概率,根据长流、短流被抽样时抽空的可能性不同,给出了相应的估计方法. 对于长流估计为最大概率的 $2N$ 个原始流,当抽样流数量小于 $2N$ 时,则认为其产生于最大的几个. 对于短流可利用其重尾分布特性,通过最小二乘法求解. 通过时间复杂度分析,可以看出所提出的方法要比现有的EM算法用更少的时间. 通过实验也表明所提出的算法的估计精度与EM算法相当,或更好于EM算法.

进一步的工作可以在以下几个方面展开:①确定原始流超时与抽样流超时之间的关系,即当原始流超时确定后,如何确定抽样流超时的时间,以及与抽样比例值 $p$ 的关系;②估计精度与抽样比例值 $p = 1/N$ 之间的关系,即估计精度确定时,抽样比例值在什么范围内可满足要求,以及满足要求的最大的 $N$ 值.

## 参考文献(References)

[1] Roberts J W. Traffic theory and the Internet [J]. *IEEE Communications Magazine*, 2001, **39**(1): 94-99.

[2] Claffy K C, Polyzos G C, Braun H W. Application of sampling methodologies to network traffic characterization [C]//*Proc of ACM SIGCOMM* '93. New York: ACM Press, 1993: 194-203.

[3] IETF. Packet sampling (psamp)[EB/OL]. (2005-02-02)[2005-06-30]. http://www.ietf.org/html.charters/psamp-charter.html.

[4] Duffield N G, Grossglauser M. Trajectory sampling for direct traffic observation [J]. *IEEE/ACM Trans on Networking*, 2001, **9**(3): 280-292.

[5] Duffield N G, Grossglauser M. Trajectory sampling with unreliable reporting [C]// *IEEE INFOCOM* 2004. Hong Kong, 2004: 1570-1581.

[6] Cisco. Sampled Cisco [EB/OL]. (2002-12)[2005-06-30]. http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide 09186a 0080081201.html.

[7] Brownlee Nevil. NeTraMet Version 4.4 [EB/OL]. (2002-12)[2005-06-30]. http://www2.auckland.ac.nz/net/Accounting/ntm.Release.note.html.

[8] Estan C, Varghese G. New directions in traffic measurement and accounting: focusing on the elephants, ignoring the mice [J]. *ACM Transactions on Computer Systems*, 2003, **21**(3): 270-313.

[9] Hohn N, Veitch D. Inverting sampled traffic [C]//*Internet Measurement Conference* 2003. New York: ACM Press, 2003: 222-233.

[10] Duffield N G, Lund C, Thorup M. Properties and prediction of flow statistics from sampled packet streams [C]// *Proc of ACM SIGCOMM Internet Measurement Workshop* 2002. New York: ACM Press, 2002: 159-171.

[11] Duffield N G, Lund C, Thorup M. Estimating flow distributions from sampled flow statistics [J]. *IEEE/ACM Transactions on Networking*, 2005, **13**(5): 325-336.

[12] Claffy K C, Braun H W, Polyzos G C. A parameterizable methodology for internet traffic flow profiling [J]. *IEEE Journal on Selected Areas in Communications*, 1995, **13**(8): 1481-1494.

[13] 陆璇. 应用统计[M]. 北京:清华大学出版社,1999: 80-89.