计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(6): 1010-1017, 2011

一种基于数据流计数的概率衰落大业务流识别方法

李 臻[1,2] 杨雅辉[1] 谢高岗[2] 覃光成[3]
[1](北京大学软件与微电子学院 北京 102600)
[2](中国科学院计算技术研究所 北京 100190)
[3](解放军理工大学通信工程学院 南京 210007)
(lizhen001@pku.edu.cn)

An Identification Method Combining Data Streaming Counting with Probabilistic Fading for Heavy-Hitter Flows

Li Zhen[1,2], Yang Yahui[1], Xie Gaogang[2], and Qin Guangcheng[3]
[1](*School of Software and Microelectronics*, *Peking University*, *Beijing* 102600)
[2](*Institute of Computing Techology*, *Chinese Academy of Sciences*, *Beijing* 100190)
[3](*Institute of Communication Engineering*, *PLA University of Science and Technology*, *Nanjing* 210007)

Abstract Identifying heavy-hitter flows in the network is of tremendous importance for many network management activities. Heavy-hitter flows identification is essential for network monitoring, management, and charging, etc. Network administrators usually pay special attention to these Heavy-hitter flows. How to find these flows has been the concern of many studies in the past few years. Lossy counting and probabilistic lossy counting are among the most well-known algorithms for finding Heavy-hitters. But they have some limitations. The challenge is finding a way to reduce the memory consumption effectively while achieving better accuracy. In this work, a probabilistic fading method combining data streaming counting is proposed, which is called PFC(probabilistic fading counting). This method leverages the advantages of data streaming counting, and it manages to find the heavy-hitter by analyzing the power-low characteristic in the network flow. By using network's power-law and continuity, PFC accelerates the removal of non-active and aging flows in table records. So PFC reduces memory consumption, and decreases false positive ratio too. Comparisons with lossy counting and probabilistic lossy counting based on real Internet traces suggest that PFC is remarkably efficient and more accurate. Particularly, experiment results show that PFC has 60% lower memory consumption without increasing the false positive ratio.

Key words heavy-hitters flow; data streaming counting; probabilistic fading; identification; method

摘 要 大业务流识别是网络监控、管理以及计费等的重要基础,网络管理者通常会对大业务流给予特别的关注.大业务流识别需要在一定识别精度的基础上有效降低资源消耗.基于PLC(probabilistic lossy counting)方法,提出了一种概率衰落的大业务流识别方法PFC(probabilistic fading counting).该方法吸取了数据流计数技术的优势,通过分析网络流量的幂律(power-law)特性和连续性,采取加快对表记录中非活动流移除力度的方式,在有效控制漏报和误报的同时,大幅度降低了存储资源开销,实现

收稿日期:2010-02-10;**修回日期**:2010-11-03
基金项目:国家"九七三"重点基础研究发展计划基金项目(2007CB310702);国家自然科学基金项目(60903208,61070237);中国科学院重大科研装备研制项目(YZ200824)

了在有限资源下对高速链路实时准确的大业务流识别.实验结果表明,与 PLC 方法相比,PFC 方法在减小误报率的同时,存储资源开销平均降低 60%以上.

关键词　大业务流;数据流计数;概率衰落;识别;方法

中图法分类号　TP393

随着 Internet 的快速发展,网络带宽不断增加,给实时网络流量监测提出了新挑战.而网络流量分布的"长尾效应"[1-5]是流量分布的重要特征,即网络中 80%的流占据了 20%的网络流量,而 20%的流占据了 80%的网络流量.通常将这些对网络流量贡献较大的少数流统称为大业务流(heavy hitters),正是因为它们的存在和"长尾效应"推动了大业务流识别方法的研究和应用.

大业务流识别是网络监控、网络管理以及计费等的重要基础.网络管理者通常会对大业务流给予特别的关注[6-8].通过对这些大业务流的识别,网络管理者可以很清楚地掌握网络中占据绝大部分字节数和包个数流的分布情况.而这些信息的获得有很大的应用价值,例如可以及时发现拒绝服务攻击(DoS)、控制流量的增长趋势、合理调配网络资源和链路容量、对异常的大流用户产生告警、针对大流重新路由以减少资源开销等[9].因此大流识别方法,特别是适用于网络监控和管理需求的大业务流识别方法,就成了网络流量测量与分析中必不可少的一种方法和手段,在学术界和工业界都引起了广泛的关注与研究.

大业务流判定标准有很多,有根据速率的、有根据突发性的、还有根据持续时间的[9],本文选取的判定标准是流包个数的多少.按照这一标准,大业务流识别就可以理解为在复杂网络流量中通过记录不同流的包个数并找出超过预设门限的大流这一过程.按照这一原理,一个简单直接的大流识别方法是储存每一个流的标识并对其频数进行计数,根据频数的大小是否超过预先设定的门限值来判定是否为所要关注的大业务流.而这种办法最大的问题就是存储资源开销过大,目前的磁盘存储设备无法满足高速网络大业务流识别需要.以一个小型企业网络为例,在一条百兆链路上,以五元组来划分的流每秒新增加 3 万余个,每秒中的并发流数可以达到 10 万个,对每一条记录用于识别和计数的信息有 200 b,把这些记录信息全部保存每分钟至少需要 200 MB 的存储资源.如何能够在有限存储资源下实现大业务流的精确识别是当前大业务流识别领域面临的一个重大挑战.

本文提出的高效大业务流识别方法——PFC 是在 PLC[10]方法的基础上,通过分析网络流量的幂律分布特性和连续性,采取加快对表记录中非活动流移除力度的方式,有效降低了存储资源的开销,并实现了在有限资源下对高速链路实时准确的大业务流识别.

1　相关工作

大业务流识别方法主要分为基于采样的方法、基于数据流计数的方法和面向特定工程应用的方法等.第 1 类方法的代表主要有基于 NetFlow 采样大流识别方法[8]、基于采样和保持的大流识别方法[6]、基于周期采样的大流识别方法[11]和改进的自适应流量采样的大流识别方法[12].面向特定工程应用的大业务流识别方法是针对实用的流量控制和带宽公平性保证等工程应用提出的,其重点不在于识别的精度和准确性而更注重满足实际的应用需要,如文献[13]提出的用于流量控制的低代价大业务流识别工具,文献[14]提出的一种采用 Breahte 方法来解决网络拥塞问题的方法,方法的核心内容是基于 heavy-hitter set 的大业务流识别和处理等.这两类识别方法存储资源开销较小,但识别精度还不够理想,特别是很难在漏报和误报之间找到一个合适的平衡点,以基于周期采样的大流识别方法为例,其误报率一般在 4.5%左右,而漏报率则高达 10%[12].

为了解决上面两类方法存在的问题,基于数据流计数技术的大业务流识别方法成为近年来大业务流识别领域研究的热点.其中两个最为著名的方法是耗计数(LC)[15]和概率耗计数(PLC)[10]两种.其中,耗计数算法把一个到达的流分成几个固定大小的窗口,并对每个窗口按自然数(i)进行编号依次处理.对于窗口中的每个新流,都将在表记录(专门用于存储跟踪大流的空间,以表记录的形式存在)中建立一个新表项,对在表记录中已经存在的流则直接更新它的频数.表记录将始终关注那些少数的流,并

且能够在任意时刻输出网络流量中的大业务流. 这种算法有一个重要参数为误差边界△*error bound*,它的值为窗口编号 i 减 1,它的引入是为了解决过早地删除表记录中没有结束的大流记录而造成的频数损失. 概率耗计数算法是为了解决 LC 算法中误差边界取值过大导致存储开销和误报率较大等问题提出的,它的误差边界不像 LC 算法那样仅仅由窗口编号 i 决定并随时间线性增长,而是采用基于概率误差区间的近似算法来估计误差. 实验证明耗计数算法中的误差边界服从 power-law 分布特性,所以只要把边界误差补偿值合理地设置在大部分流能够得到足够补偿即可(如保证被过早删除的流中 95%可以得到充分补偿即可). 改进后的 PLC 算法在每一窗口结束后的存储开销上有明显降低,误报率也有所降低.

但是,PLC 和 LC 都没有考虑如何对表记录中那些在后续窗口中不会再出现的非活动流有效地进行衰减老化处理,只是对表记录中的流采取统一的老化标准,即随窗口号的增加对表记录中的记录项流频数进行减 1 操作,这就造成了在表记录中存在大量的非活动的流记录. 我们进行流量管理控制的重点是那些实时的大流,对于已经"死亡"的非活动流并不是关注的重点,但事实上这些非活动流却占用了大量的存储资源. 通过实验证实了这一点. 我们分别从 NLANR 和中国科学院计算技术研究所接入网络出口下载了多个 Trace 进行实验,为了使实验结果更具有说服力,我们统计分析了其中 10 个 trace,得到统计平均的结果如图 1 所示,并且在本实验和以下的所有章节的实验中窗口大小的设置均与引文 PLC 算法中窗口大小一致,即 $W=100\,000$.

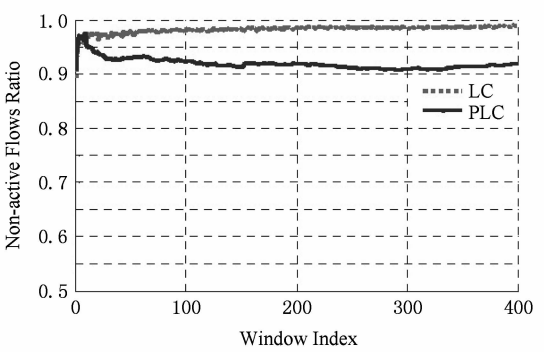


Fig. 1 The proportion of non-activity flows account for table records.

图 1 非活动流占表记录数的比例统计均值

在图 1 中,横坐标表示的是窗口号,纵坐标表示的是 10 个不同 Trace 对应窗口中非活动流所占流记录的比例取平均值的结果. 从实验统计结果中可以看出使用 LC 和 PLC 方法的表记录中非活动流占整个记录中比例取均值后仍在 90%以上,应用中对于这部分存储开销实际上是不必要的,因为它们并不是我们需要关注的大业务流.

2 概率衰落计数(PFC)方法设计

2.1 基本原理

为了解决 LC 和 PLC 方法中对非活动流衰减力度不够,致使表记录中非活动流所占比例过高,耗费大量有限存储资源的问题,本文提出了 PFC (probabilistic fading counting)算法. 该算法能够通过加大对表记录中非活动流移除力度的方式提高存储资源使用效率,其实现的关键是如何保证移除的流确实是非活动流. 为此,我们对网络中流和准大流的连续性进行了统计分析. 通过分析发现,网络中流的连续性较好,准大流的连续性更好. 直观上讲,当一个大流间隔越多个窗口不出现新数据包时,它是非活动流的可能性就越大. 该结果有利于初步建立起间隔窗口数与非活动流之间的联系. 下面,对网络中流的连续性统计分析情况进行具体介绍.

在本文中,数据流表示网络中传递信息的不同数据包的集合,按照五元组的划分标准,这些数据包属于不同的流,N 表示数据流的长度,即数据流中数据包的总个数. 在对这些数据包进行处理时,按照窗口大小 W 将数据流分割处理. 我们通过定义流的连续度 C_F 来反映流的连续性.

定义 1. 流 F 的连续度 C_F. 设 F_T 是流 F 中某一数据包所在的处理窗口索引序号,下标 T 是对流 F 中数据包按先后出现顺序进行的编号,连续度 C_F 是流 F 中相邻两个数据包出现时对应两个窗口索引号差值的最大值,即 $C_F=\max(F_T-F_{T-1})$.

由 C_F 的定义可知,连续度越小表示流的连续性越好,C_F 的值越大表示流的连续性越差,分布的窗口越分散. $C_F=0$ 表示该流在一个窗口内就结束了,$C_F=1$ 表示该流分组在窗口的分布是连续的,且至少持续了两个窗口. 同时,窗口大小对 C_F 的值有影响,对于同一组数据流,窗口的大小与 C_F 值成反相关,但是对于数据流中各个流的连续度影响是一

致的.

图 2 是我们以之前实验的 10 个 Trace 为数据源,在窗口大小 $W=100\,000$ 的情况下,进行统计得到在数据源中存在的各个流的连续度分布函数图:

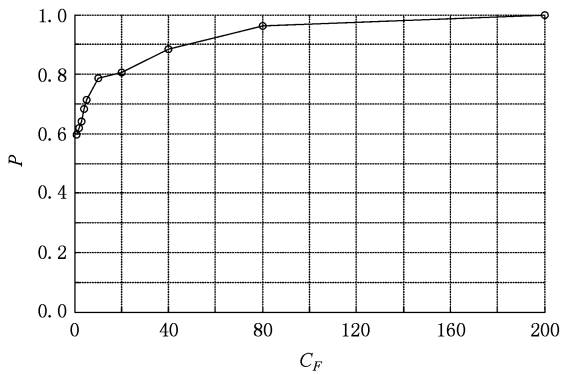


Fig. 2　Continuity distribution function.

图 2　网络中所有流连续性分布函数图

图 2 中的横坐标表示流的连续度 C_F,纵坐标表示所有数据流对应不同连续度的概率分布. 通过图 2 可以看出实验统计的 10 个 Trace 中 70%的流 C_F 值小于 5,80%的流 C_F 均值小于 20.

我们进一步分析数据流中的准大流情况,根据引文中 PLC 算法的判决标准,一般认为一个流的数据包个数如果超过数据流包总数 0.05%即为大业务流,为此,我们统计分析了上面 10 个 Trace 中数据包个数超过包总数 0.01%的流的连续分布特性,其连续性分布函数图如图 3 所示:

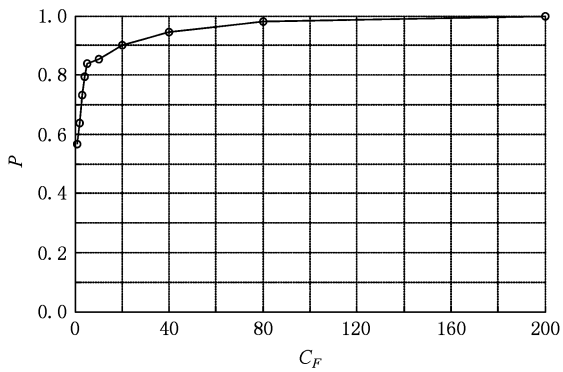


Fig. 3　Continuity distribution function of initial heavy-hitter flows.

图 3　准大流连续性分布函数图

由图 3 可以看出,80%左右的准大流连续度都小于 5,90%的准大流连续度都小于 20,这说明准大流的连续性比所有流的连续性更好.

通过上面的实验统计,可以看出网络中流的连续性较好,准大流的连续性较正常流的连续性更好. 如果像 PLC 和 LC 方法那样,仅采用使表记录中频数随窗口的增加而减 1 的方式来衰减旧流,将使得很多非活动流在表记录中持续较长时间,耗费了大量的存储资源. 因此对非活动流进行快速的衰落,将减少其在表记录中存活时间,降低表记录中记录条目,提高存储资源使用效率.

2.2　基本结构

通过上面的分析,我们提出的 PFC 方法的系统架构如图 4 所示. 对于到来的数据包,PFC 方法借鉴 PLC 方法的思想,首先依据预设窗口的大小对其进行划分和扫描,并将结果记录到表记录中. 与 PLC 方法不同的是 PFC 在表记录中加入了流状态变量,通过该变量可以标识流在网络中的状态,进而对表记录中的记录项有选择地删减. 对不断有新包到达的流记录项采用 PLC 方法进行删除,对没有新包到达的流记录项则随着时间的延长逐渐加大删除力度,减少表记录中非活动流的数目,提高资源使用效率,降低误报率.

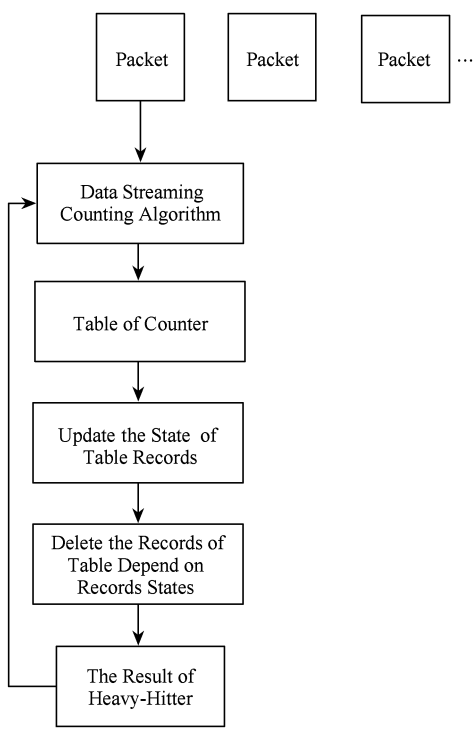


Fig. 4　System architecture of PFC scheme.

图 4　PFC 方法系统架构图

2.3　方法描述

在详细介绍 PFC 方法之前,首先给出以下标识定义,如表 1 所示:

Table 1 Symbols Used in This Paper

表 1 文中使用的符号列表

Denotation	Description
W	Window size
ε	Error parameter
i	Window index
j	Data stream packets sequence number
e	Packets
K	The number of last item in table records
N	Length of the input stream
Δ	Error bound
d_f	Flow state marking
$\hat{c}$	Estimated frequency
f_h	Threshold number of the Heavy-Hitter flow packages

对于数据流分组$\{e_j \mid 1 \leqslant j \leqslant N\}$,其中$e_j$为数据流中的数据包,$N$为数据流的数据包总数.设$s \in (0,1)$为大流包个数占数据流包总数的比例,则$f_h = sN$为大流包个数门限.设定窗口大小$W = \left\lceil \frac{1}{\varepsilon} \right\rceil$,每个处理窗口索引号为$i$,$1 \leqslant i \leqslant \left\lceil \frac{N}{W} \right\rceil$.流表记录开始为空,表记录项为四元组$(e, \hat{c}, \Delta, d_f)$,其中$d_f$为流状态标识.表记录中计数器的初始值为0,依窗口顺序对窗口内每一个数据包采用数据流计数技术对其进行扫描,若某数据包所属的流已经存在于表记录中,则对表记录中对应流的包个数记录估计频数$\hat{c}$加1,且把d_f置为0;若某数据包所属的流在表记录中不能够匹配到,则在表中建立新的插入$(e, \hat{c}, \Delta, d_f)$,且$\hat{c}$的初始值为1,$d_f$的初始值为0;对于那些在表记录中存在,而在新窗口中不存在的流记录,则更新其状态数值,更新函数如下:

$$d_f = \begin{cases} d_f + 1, & \text{新的处理窗口中没有,} \\ 0, & \text{新的处理窗口中存在,} \end{cases} \tag{1}$$

更新结束后,依据以下规则对流表记录进行移除操作.对于$d_f = 0$的活动流,依据PLC的移除规则删除那些$\hat{c} + \Delta \leqslant i$的流;对于状态数值$d_f > 0$的流,依据$\hat{c} + \Delta - D \leqslant i$规则移除表记录中的记录,其中误差边界补偿$\Delta$采用PLC的计算方法:

$$\Delta = \sqrt[\beta]{\delta(1-(i-1)^{\beta}) + (i-1)^{\beta}}, \tag{2}$$

状态衰落函数为

$$D = d_f \times s \times W, \tag{3}$$

式(3)中$s \times W$表示符合大流标准的流在一个窗口中应到达的包个数,流状态标识d_f表示这个流连续d_f个窗口没有出现,由此状态衰落函数D则表示一个流若要符合事先确定的大业务流标准在连续d_f个窗口中应达到却没有出现的包个数.此外,状态衰落函数$D = d_f \times s \times W < i \times s \times W$,其中$i$表示当前窗口编号,$i \times s \times W$表示截止当前窗口符合大业务流标准应达到的包个数.这样设定状态衰落函数,既有效地衰减了那些进入表记录中非活动流,同时又保证进入表记录中的流不会因为个别窗口中出现间断就被误删,运行过程中对非活动流的删除是随间断时间的增加不断加大力度的,直到它不再满足大流门限值时才进行最终删除,有效控制了PFC方法漏报的发生.

3 实验验证

在实验验证部分,将从存储开销的大小、平均相对误差以及系统的误报率和漏报率等几个方面来对PFC,PLC和LC方法进行比较.

定义 2. 存储开销是指每一窗口结束后表记录中的记录数,它反映了方法在运行过程中对存储资源的消耗情况.

定义 3. 流大小估计偏差也被称作平均相对误差[15],即表记录中流大小(在本文中对应流中所包含的包个数)的估计值和真实值之差与流大小的真实值之比,其主要是用来衡量不同方法对识别出的大流大小估计的准确性.

定义 4. 误报率是指在大业务流识别过程中本不是大流却被误判成大流的概率.

定义 5. 漏报率是指在大业务流识别过程中本是大流却未被识别的概率.

在这部分实验中,我们利用从NLANR和中国科学院计算技术研究所接入网络出口的获取的多个Trace进行实验,实验中均得到了较为理想的结果.由于篇幅限制,这里我们仅选取中国科学院计算技术研究所实际采集的数据集Trace1(ICT-09-08-24)和NLANR的数据集Trace2(NLANR-02-08-14)[16]进行说明.数据集属性如表2所示:

Table 2 The Information of Network Data Source

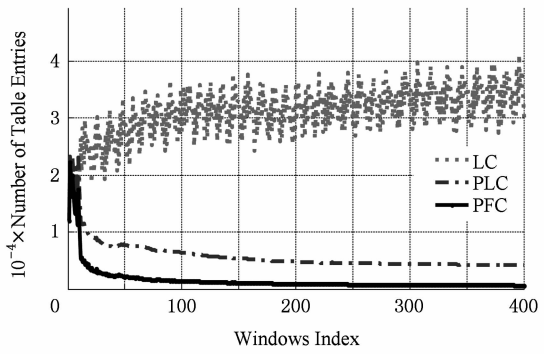
表 2 网络数据源属性信息

Datasets	Date	Packets	Flow Records
Trace1 ICT-09-08-24	2009-08-24	40 000 000	4 350 000
Trace2 NLANR-02-08-14	2002-08-14	40 000 000	646 000

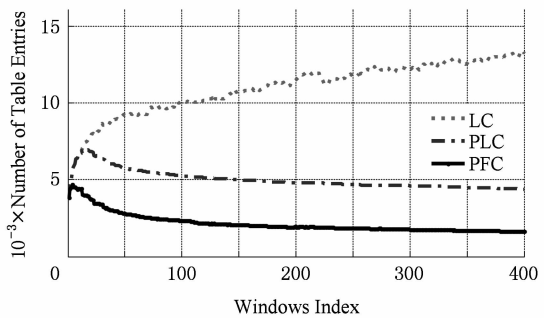
在参数的选择上,我们继续与引文 PLC[11] 保持一致,参数 S 和 ε 分别选取了 0.000 5 和 0.000 001.

3.1　存储开销的比较

PFC,PLC 和 LC 方法存储开销的情况对比如图 5 所示,其中横坐标表示窗口号,纵坐标表示对应窗口存储开销的大小:



(a)　Trace1



(b)　Trace2

Fig. 5　Memory consumption comparison.

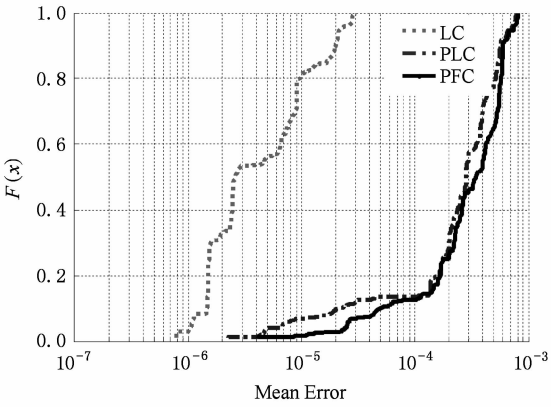
图 5　存储开销情况比较

从图 5 可以看出,采用 LC 方法表记录中的记录数随着时间的延长记录数不断上涨,而采用 PLC 和 PFC 方法表记录数随时间的延长逐渐降低并趋于稳定.出现这样的结果就像前面分析的那样 LC 方法在运行的后期由于误差补偿过大导致在表记录中存在了大量的非大流,PLC 和 PFC 采取概率误差估计补偿,通过控制误差补偿值减少了非大流在表记录中的数量.此外,还可以看出在 PLC 的基础上进行改进的 PFC,其存储资源整体上开销减少了 60%左右,这也证实了 3.1 节中对于全部流与准大流的连续性分布的分析.

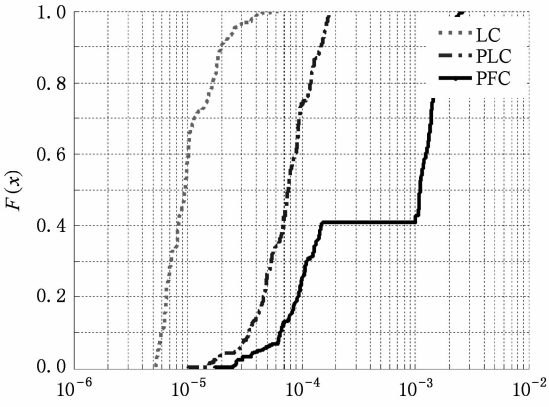
3.2　流大小估计偏差比较

流大小估计偏差实验结果如图 6 所示,其中横坐标表示流大小估计偏差,纵坐标表示对应估计偏差的概率分布函数.

从图 6 可以看出,PFC 方法在对大流大小估计上要略逊于 LC 和 PLC.这是由于在方法中引入了



(a)　Trace1



(b)　Trace2

Fig. 6　Current size of the estimation error.

图 6　流大小估计偏差

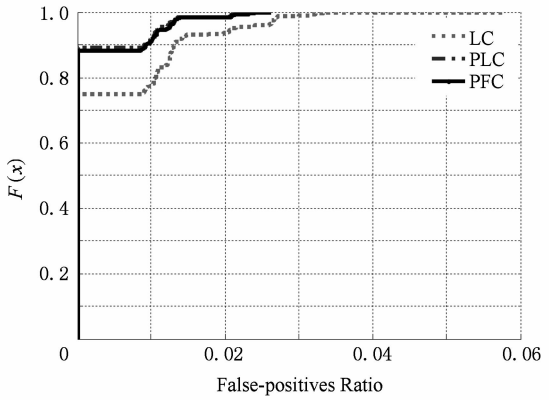
快速衰弱,从而影响到流大小的估计值.但是 PFC 方法引入的偏差是可忽略的,由于:1)PLC 和 LC 方法流大小估计偏差本身就很低,PLC 控制在 0.000 1 左右,LC 控制在 0.000 09 左右;2)从整体分布上看,Trace1 中 PFC 的平均误差和 PLC 的平均误差基本一致,Trace2 中 FPC 的平均误差只是略高于 PLC 和 LC,且数量级别控制在 0.1%以内;3)PFC 的平均误差始终低于 0.05%.

考虑到该方法是想找出大流,以便于更好进行流量控制,至于大流的具体细节属性,如大小、速率等,并不是我们的关注点.因此,FPC 是可用于实际应用环境中的.

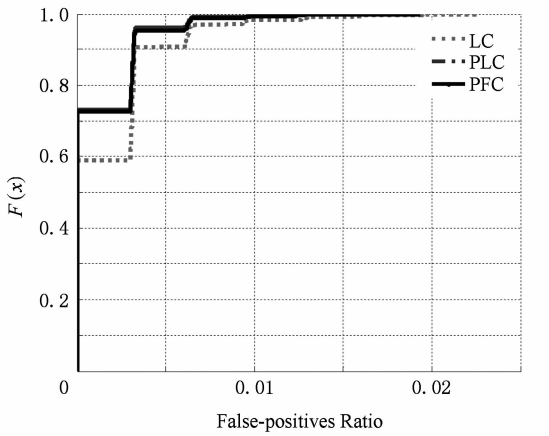
3.3　误报率和漏报率

误报和漏报是衡量识别方法的两个重要指标.如图 7 所示,横坐标表示误报的大小,纵坐标表示对应的概率分布.

从图 7 中可以看出,采用 PFC 方法的误报率低于 PLC 和 LC 方法.从误报率的统计结果上看,在 Trace1 中,PFC 方法中的大流 90%左右的误报率



(a) Trace1



(b) Trace2

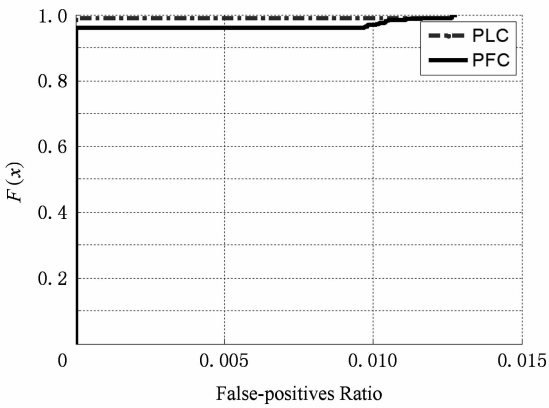
Fig. 7 The statistics of false-positives ratio.

图 7 误报率统计

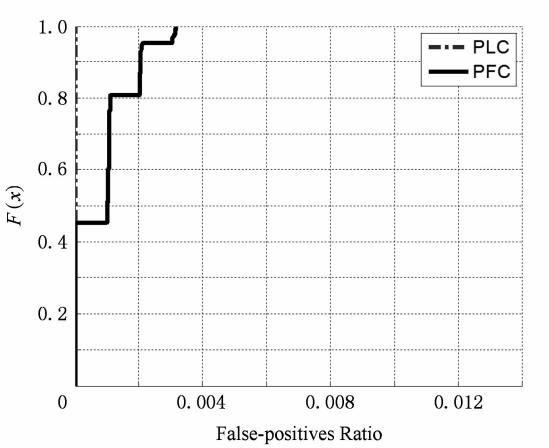
几乎控制在 0;在 Trace2 中,PFC 方法处理过的大流 72%的误报率为 0. 从误报率的大小上看,从 Trace1 和 Trace2 中发现识别的大流 99.5%的大流误报率都低于 1.5%.

在漏报方面,从实验结果看,与 PLC 方法相比漏报基本一致,PFC 漏报率情况如图 8 所示.

图 8 中横坐标表示漏报的大小,纵坐标表示对应漏报的概率分布. 在 Trace1 中,PLC 和 PFC 的漏报率基本一致,98%的大流漏报率为 0. 在 Trace2 中,采用 PFC 方法有 45%的大流漏报率为 0,80%的大流漏报率小于 0.2%,对应 PLC 方法 98%的大流漏报率为 0. 从实验结果可以看出 PFC 方法在漏报率上并没有因为加速了衰减就带来漏报率的明显提高,其漏报率与 PLC 基本一致,这是由方法的机制决定的,PFC 方法在衰减时并没有直接对表记录中的频数进行处理,而只是在进行删除判决时根据流状态函数的大小调整了删除力度,从而实现了在控制漏报的前提下有效地降低了存储资源开销.



(a) Trace1



(b) Trace2

Fig. 8 The statistics of false-negatives ratio.

图 8 漏报率统计

4 结 论

本文提出了一种在网络数据流中发现用户指定门限的大流识别方法 PFC,PFC 基于网络数据流的幂律分布特性和连续性,在 PLC 的基础上通过加快对表记录中非活动流的移除力度,使这些流以更快的速度被删除,从而有效地降低了存储资源的开销.

实验结果证明经过改进后的 PFC 方法较 PLC 方法存储资源开销能够减少 60%以上. 同时这一处理方式也使得表记录中记录项更多的是可用于实时控制的活动大流和准活动大流,为流量控制和相关工程应用创造了更好的条件.

参 考 文 献

[1] Fredj B S, Bonald T, Proutiere A, et al. Statistical bandwidth sharing: A study of congestion at flow level [C] // Proc of ACM SIGCOMM'01. New York: ACM, 2001: 111-122

[2] Mori T, Kawahara R, Naito S, et al. On the characteristics of Internet Traffic variability: Spikes and Elephants [J]. IEICE Trans Inf Syst, 2004, E87-D(12): 2644-2653

[3] Papagiannaki K, Taft N, Bhattacharya S, et al. On the feasibility of identifying elephants in internet backbone traffic, TR01-ATL-110918 [R]. St. Louis: Sprint Labs, 2011

[4] Thompson K, Miller J G, Wilder R. Wide-area internet traffic patterns and characteristics [J]. IEEE Network, 1997, 11(6): 10-23

[5] Zhang Y, Breslau L, Paxson V, et al. On the characteristics and origins of Internet flow rates [C] //Proc of ACM SIGCOMM'2002. New York: ACM, 2002: 309-322

[6] Estan C, Varghese G. New directions in traffic measurement and accounting [C] //Proc of ACM SIGCOMM'02. New York: ACM, 2002: 323-338

[7] Papagiannaki D, Taft N, Bhattacharyya S, et al. A pragmatic defition of elephants in Internet backbone traffic [C] //Proc of the 2nd ACM SIGCOMM Internet Measurement Workshop. San Francisco: Morgan Kaufmann, 2002: 175-176

[8] Estan C, Keysy K, Moore D, et al. Building a better NetFlow [C] //Proc of ACM SIGCOMM'04. New York: ACM, 2004: 245-256

[9] Kun C L, John H. On the correlation of Internet flow characteristics, ISI-TR-574 [R]. Los Angeles: Information Sciences Institute, University of Southern California, 2003

[10] Dimitropoulos X, Hurley P. A Kind. Probabilistic lossy counting: An efficient algorithm for finding heavy hitters [J]. ACM SIGCOMM Computer Communication Review. 2008, 38(1): 7-16

[11] Mori T, Uchida M, Kawahara R. Identifying elephant flows through periodically sampled packets [C] //Proc of IMC'04. New York: ACM, 2004: 115-120

[12] Wang Dan, Xie Gaogang, Yang Jianhua, et al. An inproved adaptive sampling method for traffic measurement [J]. Journal of Computer Reserach and Development, 2007, 44(8): 1339-1347 (in Chinese)
(王丹, 谢高岗, 杨建华, 等. 一种改进的自适应流量采样方法[J]. 计算机研究与发展[J]. 2007, 44(8): 1339-1347)

[13] Lu Y, Bonomi F. ElephantTrap: A low cost device for identifying large flows [C] // Proc of the 15th IEEE Symp on High-Performance Interconnects. Piscataway, NJ: IEEE, 2007: 99-108

[14] Chang W C, Lin B. A simple mechanism for throttling high-bandwidth flows [G] //Research Letters in Communications. New York: Hindawi Publishing Corporation, 2008: 1-5

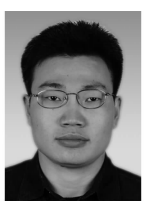
[15] Manku S G, Motwani R. Approximate frequency counts over data streams [C] //Proc of the 28th Int Conf on Very Large Data Bases (VLDB). San Francisco: Morgan Kaufmann, 2002: 346-357

[16] NLANR: A blilene-I data set [OL]. [2010-11-01]. http://pma. nlanr. net/Traces/long/ipls1. html(SHIJI)

Li Zhen, born in 1984. ME candidate. His main research interests include network measurement and evaluation, internet application technology.

Yang Yahui, born in 1966. PhD and associate professor. Her main research interests include network and security management, network measurement and evaluation, internet application technology.

Xie Gaogang, born in 1974. Professor and PhD supervisor of the Institute of Computing Technology, Chinese Academy of Sciences. Senior member of China Computer Federation. His main research interests include future internet, network measurement and modeling.



Qin Guangcheng, born in 1985. PhD candidate. His main research interests include information distribution, wireless sensor network, network measurement, Ad hoc network.