doi:10.3969/j.issn.1000-436x.2014.10.014

基于同源组合布鲁姆过滤器的早期流量抽样算法

侯颖，郭云飞，黄海，王凯
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：提出一种同源组合布鲁姆过滤器结构，该结构包含流抽样（sample）和分组计数（packet）2 个计数器向量组合，2 个计数器向量宽度不同，以相同的散列源函数计算散列位置。基于该结构设计的早期流量抽样算法利用 2 个计数器向量将流抽样判断与分组计数检测分开，避免了早期流量抽样中大量抽样已经结束的流对分组计数过程的影响。分析和实验结果表明，通过调节 2 个计数器的宽度比 α，在不增加内存空间的条件下，该算法有效降低了误判率。

关键词：流量抽样；布鲁姆过滤器；组合布鲁姆过滤器；长度调节因子
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)10-0117-10

Early traffic sampling algorithm based on SSCBF

HOU Ying, GUO Yun-fei, HUANG Hai, WANG Kai
（National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, Henan，450002,China）

Abstract: An early traffic sampling algorithm was proposed based on same source and combination Bloom filter (SSCBF), a structure with two Bloom filters: flow-sampling vector and packet-count vector. The hash functions of the two vectors were same but the counters' widths were different. This structure separated the sampling judgment and the packets counting. That could avoid the interference with packet count vector by the finished sampling flows. The false positive rate of the algorithm and an adjustable parameter α, ratio of the two vectors' widths, were analyzed. The analysis and experiments demonstrate that with suitable α, the algorithm can achieve higher accuracy without increasing the space complexity.

Key words: traffic sampling, Bloom filter, combinational Bloom filter, length adjustable factor

1 引言

在线流量分类也称为早期流量分类，是网络监测、管理和预警的重要基础技术。流建立初期的数据分组在流量管理，尤其是在线流量分类中非常重要。研究者通常利用流建立初期的少量数据分组，计算流统计特征进行在线流量分类[1]。文献[1]用统计的方法证明只需要提取流开始的前 4 个数据分组，即可得到比较高的平均流量分类准确性。随着骨干网带宽的不断增长，提取完整网络流量和流统计特征的资源消耗和计算代价急剧增加。因此，通过早期流量抽样，仅采集流建立初期的数据分组，能够以较低的开销获得在线流量分类的基础数据。

早期流量抽样属于流量测量研究领域，与经典的均匀随机抽样和固定周期抽样等流量抽样方法不同，早期流量抽样定义如下。

定义 1 流 S 的数据分组序列 $\{s_1,s_2,s_3,\cdots,s_N,s_{N+1},\cdots,s_M\}$ 为抽样分组数，以概率对 p_i 流 S 的第 i 个数据分组进行抽样，其中

$$p_i=\begin{cases}1, i\leqslant N\\ 0, i>N\end{cases} \tag{1}$$

收稿日期：2014-04-10；**修回日期**：2014-09-25
基金项目：国家自然科学基金资助项目(61309019)；国家高技术研究发展计划(“863”计划)基金资助项目(201101A103,2011AA010603)
Foundation Items: The National Natural Science Foundation of China (61309019); The National High Technology Research and Development Program of China (863 Program) (201101A103,2011AA010603)

早期流量抽样的准确性，直接决定了后续流量识别的准确度，因此早期流量抽样精度要求较高。目前早期流量抽样算法并没有取得针对性的研究成果。本文的主要贡献在于：

1) 首次提出早期流量抽样的定义；

2) 基于计数布鲁姆过滤器（NCBF, naïve-count bloom filter）结构实现早期流量抽样，并结合早期流量抽样的特点从误判概率、时间复杂度和空间复杂度等方面分析了算法的性能；

3) 利用公开的被动型测量数据，验证了早期流量抽样中抽样结束率的取值规律；

4) 提出同源组合布鲁姆过滤器（SSCBF, same source and combination bloom filter）结构，并基于此结构设计了早期流量抽样算法，分析并验证了算法的误判概率、时间复杂度和空间复杂度。

2 相关研究

在高速流量测量领域，通常利用流量抽样方法对原始流量进行估计，如已经成为业界标准的 Cisco 公司生产的 NetFlow 设备[4]，使用固定周期采样的方法。文献[5]设计了一种草图指导的公平抽样（SGS, sketch guided sampling）算法，以当前流的分组数量的单调递减函数为依据，设置报文抽样概率，即通过牺牲长分组抽样率以换取中、小流的分组抽样率。但是显然无论固定周期采样还是其他概率的分组抽样方法，都不能准确抽取所有数据流的开始几个数据分组，因此不能应用于早期流量抽样。

在高速网络中进行早期流量抽样面临的核心问题在于：如何快速且准确地定位和记录每个网络流的抽样信息。最直观的方法是逐流建立流表结构，根据流表记录的报文数量确定是否进行抽样。这种方法原理比较简单，但是为了定位流表，需要保留每个流的五元组信息，占用空间较大，而且通过散列函数定位流表，散列冲突时需顺序查询冲突链表，开销较高，不适合在高速网络中使用。

为了节省存储空间同时提高处理效率，文献[6]提出利用最近最久未使用（LRU, least recently used）算法进行大流检测，其思想是利用链表结构维护活跃流状态，当新流到达时将最久未到达数据分组的流替换出去，由于大流数据分组频度高，能够一直保存在链表当中。文献[7]在 LRU 的基础上增加了一级布鲁姆过滤器，分离了大流判断和大流过滤。该类算法不用维护所有流状态信息，减少了占用的内存空间。但是该类长流检测算法链表上保留的活跃长流，大部分是早期流量抽样中已经结束抽样的流，而早期流量抽样中正在抽样的慢流在链表空间中容易被替换出去。此外，该类算法同样需要利用散列函数定位流表，应用于早期流量抽样时，没有解决占用空间大和查询效率低的问题。

为了克服按流维护流表结构的效率问题，很多大流检测算法采用概要数据结构对流的报文数量进行统计，如 MF(multistage filter)[8]和双重 CBF (counter Bloom filter)[9]等。MF 算法由 Estan 等人提出，是应用多级过滤器对每个报文进行更新计数，如果每级过滤器相应的计数器都超过了预设定的阈值，则认为该流是大流。该方法与计数布鲁姆过滤器 NCBF (Naïve-CBF)的原理一致。文献[9]中提出基于双重 CBF 的算法(简称 CCBF)进行大流识别和抽样，将大流过滤和大流存在分开进行处理，但是该算法 2 个布鲁姆过滤器采用相同大小的计数器空间，与 NCBF 相比，在占用相同存储空间条件下准确度有所下降。

布鲁姆过滤器作为一种高效简洁的概要数据结构，在网络流量处理中被广泛应用，但是该结构的查询准确率与元素密度（集合元素数量与布鲁姆过滤器计数器数量的比值）负相关。在高速链路中，数据速率高，并发流量数量大，而受制于成本因素，很多采用专用处理器或 ASIC(application specific integrated circuit)的流量处理系统内部存储空间有限，导致 CBF 结构的元素密度过大，影响算法准确率。因此如何在有限存储空间情况下提高基于布鲁姆过滤器算法的准确率，是研究的重要内容。

3 基于 NCBF 的早期流量抽样算法

计数型 Bloom filter 称为 Naïve-CBF，是由 Fan 等人在文献[10]中提出的。其定义如下：集合 $S=\{s_1,s_2,\cdots,s_n,\}$ 共有 n 个元素，通过 k 个 Hash 函数 $h_1,h_2,\cdots,h_k$ 映射到长度为 m 的向量 V 中，向量 V 的每一维设置成一个计数器，记为 NCBF[i]，初始值设为 0。每一个 Hash 函数相互独立且函数的取值范围为{0, 1, 2,…, m−1}。

集合到向量 V 的映射过程如下：当元素插入集合 S 时，对于每一个元素 s_i，计算 $h_j(s)(1\leqslant j\leqslant k)$，令 NCBF[$h_j(s)$]加 1，即向量对应位置计数器加 1；当元素 s_i 删除时，则向量对应位置计数器减 1；当查询元素是否属于集合 S 时，对于给定的元素 x，

检查向量 V 的 k 个位置 NCBF$[h_j(x)],(1 \leqslant j \leqslant k)$ 是否为 0。判断如果其中有一个为 0，则 x 一定不在集合 S 中；若全部值均不为 0，则 x 可能属于集合 S。实际应用中，可以根据集合元素的增加与删除的统计规律，选择适当的计数器大小，防止计数器的溢出。

图 1 为基于 NCBF 结构的早期流量抽样算法。假设 N 为每流抽样的数据分组数量，基于此 NCBF 结构的早期流量抽样算法的主要过程如下。

1) 提取报文的流标识（五元组：源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议类型），作为散列函数的输入，得到 k 个 $h_j(s)(1 \leqslant j \leqslant k)$。

2) 将 k 个散列值映射到计数器向量中，并取最小值，即 $b = \min(\text{NCBF}[h_j(s)]), j = 1,2,\cdots,k$，作为已经抽样的数据分组个数的估计值[11,12]，如果 b 大于阈值 N，则不抽样，否则进行抽样，并且计数器加 1。

3) 判断流是否结束，如果结束，则所有此流对应的计数器减去 b。

图 2 给出了 NCBF 算法中在第 N(N=4)，分组到达时和流结束后计数布鲁姆过滤器的变化情况。由图 2 可以看出，当流结束时，此流对应的计数器向量均减少了 N。

4　基于 SSCBF 的早期流量抽样算法

由于网络流量有一定的持续性，已完成早期抽样的流占线路上并发流数量的绝大部分，而为了判断是否抽样，在整个流的生命周期中，NCBF 的计数器必须一直保持有效，导致集合元素密度高，抽样准确率降低。因此考虑将已抽样流和正在抽样的流采用不同长度的存储空间分别进行统计，最终在占用相同存储空间的情况下，提高算法准确率。

4.1　抽样结束比率分析

本节通过实际流量分析早期流量抽样时，并发流量中已结束抽样流数目与正在抽样流数目的比率关系。首先定义抽样结束比率 R 为线路上已抽样结束流数量与并发流数量的比率。假设网络中 n 个并发流，其中 n_1 个流为已抽样结束的流，n_2 个流为正在抽样的流，且 $n = n_1 + n_2$。则抽样结束比率为

$$R = n_1/n \tag{2}$$

本文选择美国国家实验室 NLANR（national laboratory for applied network research）公开的被动型测量数据[13]为数据源进行仿真实验，实验用数据源文件为 ERF 格式，流量数据分组包括两组，分别采自新西兰的某个 ISP 和 Waikato 大学校园网，利用 DAG3.7GE 卡进行连续分组采集。为保护用户隐私，流量数据中仅仅包含数据分组的头部。ISP 流量持续时间为 30 min，校园网流量持续时间为 24 h，为了便于比较，Waikato 校园网的数据只提取了前 30 min 左右的流量数据进行分析。原始流量数据的详细信息如表 1 所示。

图 3 为 New Zealand ISP 数据集在抽样阈值 N 分别为 4、5、6、7 时，抽样结束率随时间的变化趋势。图 4 为 Waikato network 数据集在抽样阈值 N 分别为 4、5、6、7 时，抽样结束率随时间的变化趋势。从图中可看出，在采集初期，抽样结束率较低，随着时间推移，该比率迅速增加到 0.9 以上，然后在 0.9~1 之间基本保持平衡状态。

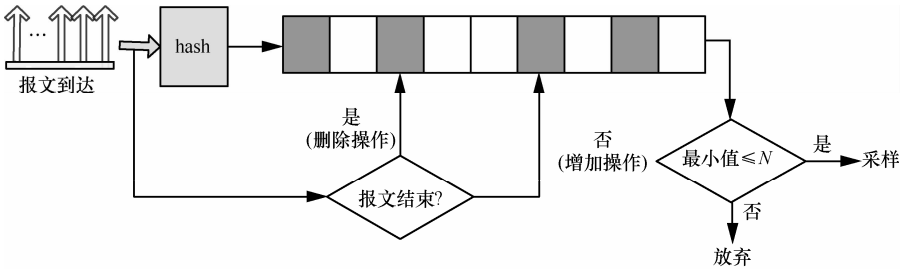


图 1　NCBF 早期流量抽样算法

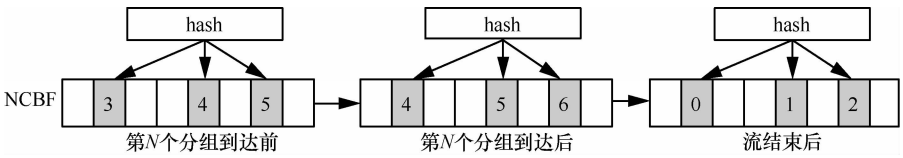


图 2　N=4 时，第 4 分组到达及结束后 NCBF 的变化

表 1　仿真实验流量数据的详细信息

数据来源	流量数据名称	持续时间/min	总流数	总分组数
New Zealand ISP	20090105-220000-0.dsl	30	1 037 043	21 338 813
Waikato network	20110407-000000-0	30	817 893	10 388 222

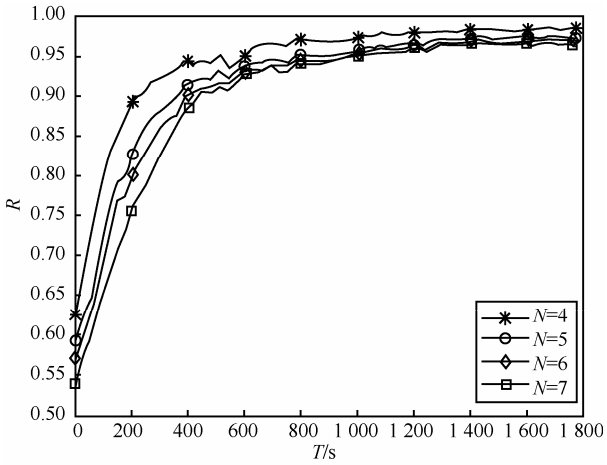


图 3　New Zealand ISP 数据集在不同抽样阈值下抽样结束率

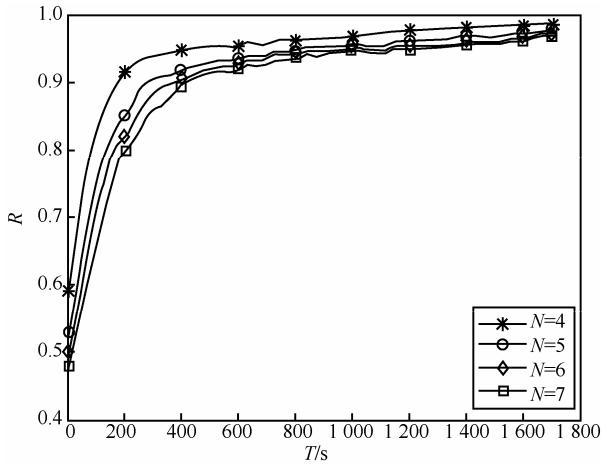


图 4　Waikato network 数据集在不同抽样阈值下抽样结束率

根据对上述网络的数据分析，可以得出早期流量抽样时的抽样结束比率取值规律：在网络中，相对于流的整体长度，早期流量抽样的抽样阈值 N 较小，因此已结束抽样流数目远大于正在抽样流数目，其抽样结束比率在稳态时取值区间通常为 0.9~1 之间。基于上述分析，本文提出 SSCBF 算法，将已抽样流和正在抽样的流采用不同长度的存储空间分别进行统计，在占用相同存储空间的情况下，提高抽样的准确率。

4.2　SSCBF 算法描述

同源组合布鲁姆过滤器定义如下：集合 $S=\{s_1,s_2,\cdots,s_n\}$ 共有 n 个元素，通过 k 个散列函数 $h_1,h_2,\cdots,h_k$ 分别映射到向量 V_1 和 V_2 中，向量每一维均设置为一个计数器，其中向量 V_1 的长度为 m_1，向量 V_2 的长度为 m_2。2 个向量长度满足

$$m_2=\alpha m_1 且 \alpha<1 \tag{3}$$

其中，α 为长度调节因子。

SSCBF 与 NCBF 的区别如图 5 所示。NCBF 只有一个计数器向量 V，而 SSCBF 存在 2 个不同长度的计数器向量 V_1 和 V_2，将分组计数与流抽样判断分开。2 个计数器向量采用同样的散列算法计算散列位置。SSCBF 中 2 个计数器向量分别称为：sample 和 packet。其中 sample 用于标记已完成早期抽样的流，向量的长度设为 m_1，packet 用于对流数据分组进行计数，向量的长度设为 m_2。

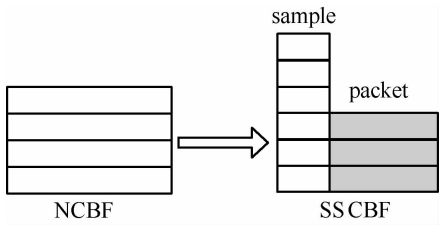


图 5　SSCBF 结构

根据 3.1 节分析，已完成早期抽样的流占线路上并发流数量的绝大部分，需要进行分组计数的流占比很小，因此可以在不影响整体误判率的情况下，将 packet 向量的长度 m_2 适当减小；另一方面，由于 sample 向量计数器只是作为抽样标记，不记录已抽样分组数量，其计数器位宽可以适当减小，对应的 sample 计数器向量长度 m_1 增大。通过选择合理的长度调节因子 α，在占用相同的存储空间条件下，降低算法的整体误判率。图 6 为 SSCBF 流抽样结构。

假设 N 为每流抽样的数据分组数量，SSCBF 算法的主要过程如下。

1) 当一个报文到达时，提取流标识（五元组：源 *IP* 地址、源端口号、目的 *IP* 地址、目的端口号、协议类型），作为散列函数的输入，得到 k 个散列值 $h_j(s),1\leqslant j$。

2) 将 $h_j(s)$按照 sample 向量长度取模，直接映

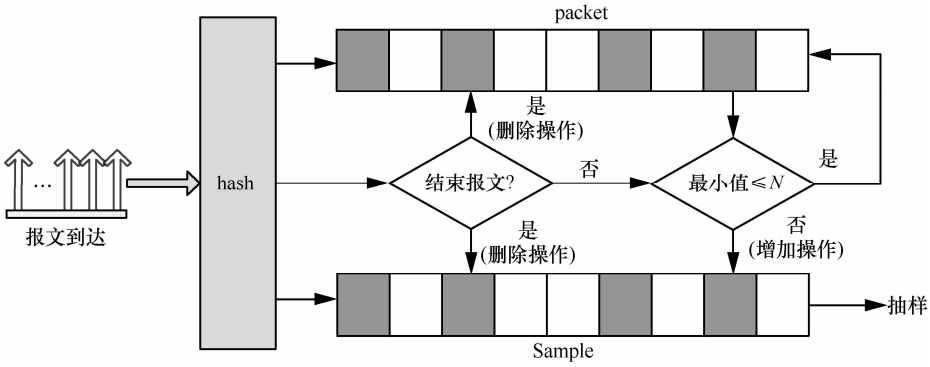


图 6　SSCBF 流抽样结构

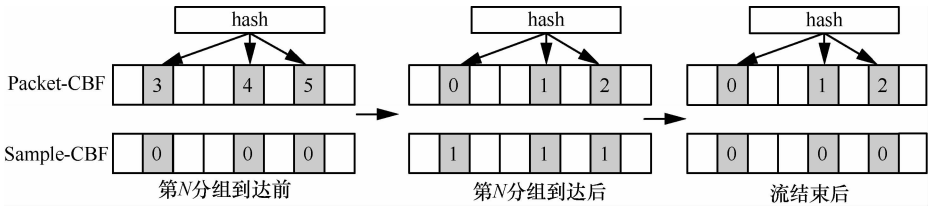


图 7　N=4 时，第 4 个分组到达及结束后 2 个计数器向量的变化

射到 sample 向量中，如果 k 个映射结果均非 0，则该报文不需抽样。

3) 如果抽样，将 $h_j(s)$按照 packet 向量长度取模，映射到 packet 向量中，在 k 个映射结果中，取最小值，设 $b=\min(\text{packet}[h_j(s)]), j=1,2,\cdots,k$ 。

4) 如果 b 超过阈值 N，将此流写入 sample 向量，表示不再进行抽样，并且 packet 向量对应的 k 个计数器减 b。

5) 如果 b 没有达到阈值 N，则直接在 packet 向量相应的 k 个计数器加 1。

6) 判断流是否结束，如果结束，则清除此流对应的计数器向量。

图 7 说明了 sample 和 packet 2 个计数器向量在第 N 分组到达时和流结束后的变化情况。当第 N 个分组到达时，packet 对应的计数器向量减少 N，并且 sample 对应的计数器向量置 1。

5　空间复杂度分析

5.1　NCBF 的空间复杂度

布鲁姆过滤器所需空间用计数向量占用的比特总数来衡量，在向量长度 m 固定的条件下，算法占用的存储空间与单个计数器所需的位数正相关。但是，如果计数器位数设计过小，会导致计数器溢出影响误判率指标。因此，计数器位数应保证在满足误判率指标下，计数器值不会产生溢出。

计数器溢出的概率可以描述为：网络中有 n 个并发流，当新流报文到达时，在 m 个计数向量中，第 i 个计数器的值超过计数器最大值 θ 的概率。

定义 $j=\lceil \theta/N \rceil$，在早期流量抽样中由于每个流对应的计数器均会增加 N，所以 j 的物理含义为当计数器是 θ 时映射到计数器上的流个数。

第 i 个计数器的值等于 θ 的概率可以表示为

$$P\{c(i)=\theta\}=\binom{nk}{j}\left(\frac{1}{m}\right)^{j}\left(1-\frac{1}{m}\right)^{nk-j} \tag{4}$$

其中，$j=\lceil \theta/N \rceil$ ，则第 i 个计数器不小于最大值 θ 的概率，即计数器溢出概率为

$$P\{c(x)\geqslant\theta\}\leqslant\binom{nk}{j}\frac{1}{m^{j}}\leqslant\left(\frac{enk}{jm}\right)^{j} \tag{5}$$

根据文献[14]，NCBF 散列函数的个数 k 最优值为 $\ln 2m/n$，因此有

$$P\{c(x)\geqslant\theta\}\leqslant\left(\frac{e\ln 2}{j}\right)^{j} \tag{6}$$

根据式(6)，可以得到 N=4，8，16 时，不同最大值 θ 的计数器溢出概率，如图 8 所示。

早期流量抽样的应用中，抽样阈值 N 比较小，对于每流所需要数据分组通常小于 10。从图 8 可以看出，抽样阈值 N 越小，计数器溢出概率下降得越快。当抽样阈值 N 为 16，θ 为 256 时，计数器溢出概率已经达到 10^{-15}，足够满足抽样应用要求。因此，

早期流量抽样中的计数器最大值可设置为 256，对应的位宽为 8 bit。

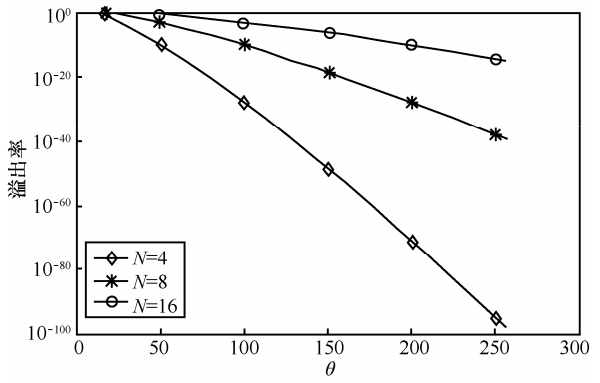


图 8 不同 N 值时计数器溢出概率

设 NCBF 计数器向量长度为 m，则根据上述分析，NCBF 算法占用空间 S 为 $8m$ bit。

5.2 SSBF 的空间复杂度

在 SSCBF 算法中，定义了 2 个计数器向量 sample 和 packet，下面分别对其计数器位宽进行分析。

由于 sample 计数器向量只是标记已抽样流，每个抽样流只导致 sample 计数器增加 1，因此根据上节分析，该计数器溢出概率满足

$$P\{c_{\text{sample}}(i)\geqslant\theta\}\leqslant\left(\frac{e\ln 2}{\theta}\right)^{\theta} \tag{7}$$

当 θ 为 16 时，计数器溢出概率为 1.37×10^{-15}，足够满足应用要求。因此，sample 计数器最大值可设置为 16，对应的位宽为 4 bit。

由于 packet 计数器向量需要记录抽样阈值，该计数器溢出概率与 NCBF 相同，根据 4.1 节分析，packet 计数器位宽设置为 8 bit。

综上，SSCBF 算法占用空间为 $4\times m_1+8\times m_2=(4+8\alpha)m_1$。

6 算法误判概率分析与验证

早期流量抽样算法的误判定义为：流 s 的第 i 个报文到达，当 $i<N$ 时，抽样概率 $p_i=0$。布鲁姆过滤器作为精简的概要数据结构，算法中存在误判概率。下面分别分析在占用相同内存空间情况下，NCBF 和 SSCBF 的误判概率。

假设 2 个算法占用的内存空间大小均为 S bit。

6.1 NCBF 误判率分析

NCBF 的误判率可以描述为：网络中有 n 个并发流，当一个新流报文到达时，在 m 个计数向量中，由 k 个散列函数计算的 k 个计数器的值均超过抽样阈值 N 的概率。

根据 4.1 节分析，对于内存空间大小为 S 的 NCBF，$m=S/8$。为简化分析，假设散列函数结果完全随机，且新流被抽样完成前，系统并发流数没有变化。则向量中某个计数器为 0 的概率 $p=(1-\frac{1}{m})^{nk}$，该概率与抽样阈值无关。此时误判的前提是该新流对应的 k 个计数器值均非 0，导致部分早期数据分组会因为计数器提前超过抽样阈值无法被抽样。因此新流的误判概率为

$$p_{\text{NCBF}}=(1-p)^k=\left(1-\left(1-\frac{1}{m}\right)^{kn}\right)^k$$

$$\approx\left(1-\mathrm{e}^{-kn/m}\right)^k=\left(1-\mathrm{e}^{-8kn/\mathrm{S}}\right)^k \tag{8}$$

图 9 是 k 分别为 3、5、7 时，p_{NCBF} 随着 S/n 的比值的变化情况，可以看出，p_{NCBF} 随着 S/n 的增大单调递减。

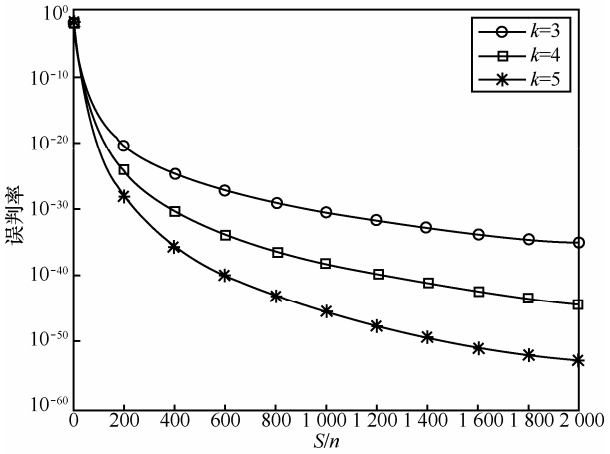


图 9 不同 k 值时，漏抽概率随 S/n 的比值变化情况

6.2 SSCBF 误判率分析

根据 3.2 节对 SSCBF 算法的描述，在 SSCBF 算法中，计数器向量 sample 和 packet 的长度分别为 m_1 和 m_2，并且 $m_2=\alpha m_1$。

根据 4.2 节的分析，对于内存空间大小为 S 的 SSCBF，m_1 和 m_2 的长度为

$$\begin{cases}m_1=S/(4+8a)\\ m_2=aS/(4+8a)\end{cases} \tag{9}$$

则当一个新流报文到达时，被误判为抽样已结束流的概率

$$p_{\text{sample}}=\left(1-\left(1-\frac{1}{m_1}\right)^{kn_1}\right)^k\approx\left(1-\mathrm{e}^{-kn_1/m_1}\right)^k$$
$$=\left(1-\mathrm{e}^{-(4+8a)kn_1/S}\right)^k=\left(1-\mathrm{e}^{-(4+8a)kRn/S}\right)^k \quad (10)$$

而在抽样计数阶段被误判为抽样结束的概率

$$p_{\text{packet}}=\left(1-\left(1-\frac{1}{m_2}\right)^{kn_2}\right)^k\approx\left(1-\mathrm{e}^{-kn_2/m_2}\right)^k$$
$$=\left(1-\mathrm{e}^{-(4+8a)kn_2/aS}\right)^k=\left(1-\mathrm{e}^{-(4+8a)k(1-R)n/aS}\right)^k \quad (11)$$

因此，SSCBF 算法的误判率为

$$p_{\text{SSCBF}}=\frac{n_1}{n}p_{\text{sample}}+\frac{n_2}{n}(1-p_{\text{sample}})p_{\text{packet}}$$
$$=\frac{n_1p_{\text{sample}}+n_2p_{\text{packet}}-n_2p_{\text{sample}}p_{\text{packet}}}{n} \quad (12)$$

相对于 p_{sample} 和 p_{packet}，$p_{\text{sample}}p_{\text{packet}}$ 可以忽略，因此得到 SSCBF 的误判率为

$$p_{\text{SSCBF}}\approx Rp_{\text{sample}}+(1-R)p_{\text{packet}} \quad (13)$$

为了研究 α 的取值与误判率的关系，取值 k=7，S/n=320，当抽样结束率 R 为 0.90、0.95、0.98 和 0.99 时，SSCBF 的误判率仿真结果如图 10 所示。由图 10 可见，R 取不同值长度调节因子 α 均存在最优值，在该值下误判率最小，随着 α 增大和减小，误判率均有所提高，取不同的 k 和 S/n 并不影响该曲线的特性。原因在于：当 α 小于最优值时，随着 packet 计数器向量长度空间变小，packet 计数器的误判随之增加，导致整体误判率上升；而当 α 大于最优值时，随着 sample 计数器向量长度空间变小，sample 计数器的误判增加，导致整体误判率上升。

另外，随着长度调节因子 α 增大，4 条曲线的误判率逐渐接近，表明此时 SSCBF 的误判率与抽样结束比率 R 弱相关。这是因为当 α 增大到一定值后，packet 计数器向量的误判对整体误判的影响很小，整体误判率主要由 sample 计数器误判造成。由于 sample 计数器向量的误判率主要由 n_1 数值决定，而 n_1 远大于 n_2，因此误判率与抽样结束比率 R 弱相关。

从图 10 可以看出，当长度调节因子 α=0.1 时，误判率与抽样结束比率 R 弱相关。此时 SSCBF 与 NCBF 误判率随 S/n 变化的比较结果如图 11 所示。由图 11 可以看出，SSCBF 的误判率整体优于 NCBF，且随着 S/n 的增加，SSCBF 和 NCBF 的误判率均随之下降，但 SSCBF 误判率下降得更快。并且，抽样结束比率 R 从 0.90 到 0.99，SSCBF 的误判率变化不大。

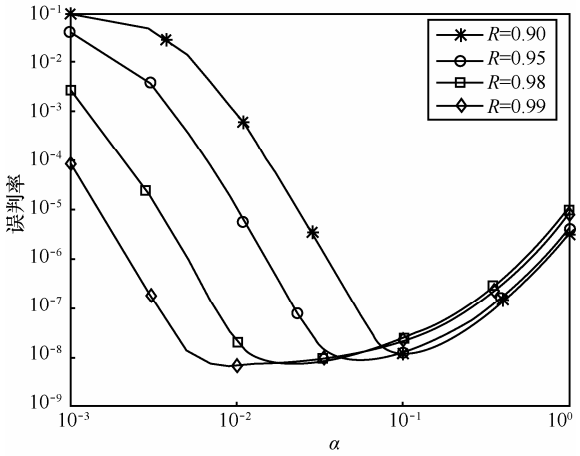


图 10　SSCBF 误判率随 α 变化情况

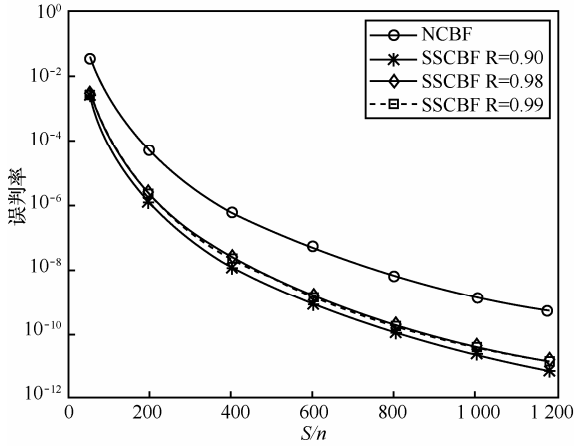


图 11　SSCBF 与 NCBF 误判率比较

6.3　算法误判概率实验

本节实验均使用 3.1 节进行抽样结束比率分析实验时的流量数据。主机运行 Windows 7 操作系统，CPU 配置为 Intel i5，主频为 2.50 GHz，配置内存为 6 GB。

1) 长度调节因子对误判率的影响

设置 k=7，早期抽样阈值 N=4，S/n 设置为 320 时，长度调节因子不同取值对 SSCBF 算法误判率的影响进行实验，结果如图 12 所示。实验结果表明：当长度调节因子小于 0.15 时，误判率随长度调节因子增大而下降，当长度调节因子大于 0.09 时，误判率随长度调节因子增大而增大，整体看来长度调节因子取值在 0.09 附近时，误判率取最小值。图

12 中长度调节因子与误判率的变化趋势与图 10 基本一致，验证了 5.2 节的分析。

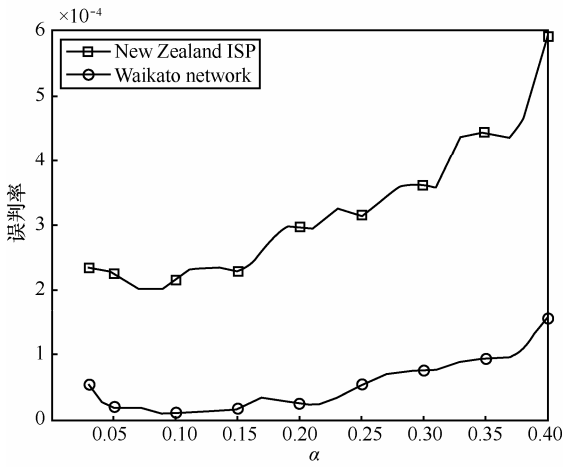


图 12　不同长度调节因子时算法误判率

2) *S*/*n* 参数对误判率的影响

设置 k=7，早期抽样阈值 N=4，长度调节因子 α=0.09 时，*S*/*n* 不同取值对 SSCBF 算法误判率的影响进行实验，结果如图 13 所示。实验结果表明：随着 *S*/*n* 取值增大，SSCBF 算法的误判率不断下降。

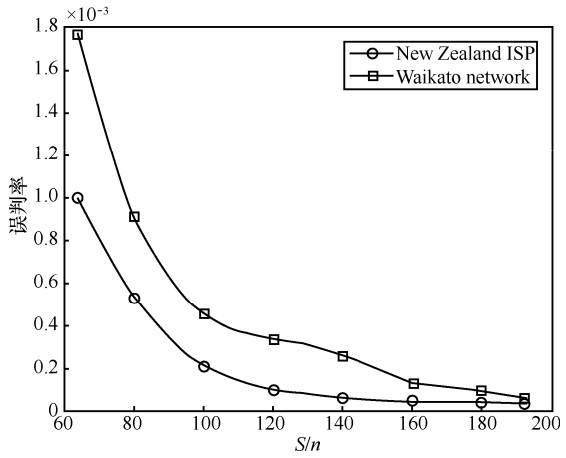


图 13 不同 *S*/*n* 时算法误判率

3) 与其他算法的比较

在占用同样存储空间情况下，选择 LRU 链表和 CBF 2 类主要的流量测量方法中的代表性算法：LRU、LRU-BF、NCBF 和 CCBF，应用于早期流量抽样并与 SSCBF 方法进行比较。数据源为 3.1 节所使用的 New Zealand ISP 数据，早期抽样阈值 N=4，散列函数设置为 7，SSCBF 的长度调节因子 α=0.09，LRU 链表中单流记录占用空间为 22 byte（五元组 13 byte、报文计数 1 byte、双向链表指针 8 byte）。算法的误判率比较结果如图 14 所示。从图中可以看出，在占用相同的存储空间条件下，SSCBF 算法的误判率指标大大优于 LRU 类算法，这是因为 LRU 类算法需要存储流的五元组和链表指针等信息，在相同存储空间下其可存放的流表记录大幅度减少，导致流反复被淘汰，影响了准确率。在 CBF 类算法中，CCBF 的误判率最高，SSCBF 的误判率最低。如内存占用为 13 MB 时，SSCBF 的误判率为 2.03×10^{-4}，NCBF 的误判率为 1.04×10^{-3}，CCBF 的误判率为 1.0×10^{-2}。因此，在占用同样内存空间条件下，与其他算法相比，SSCBF 的误判率更低。

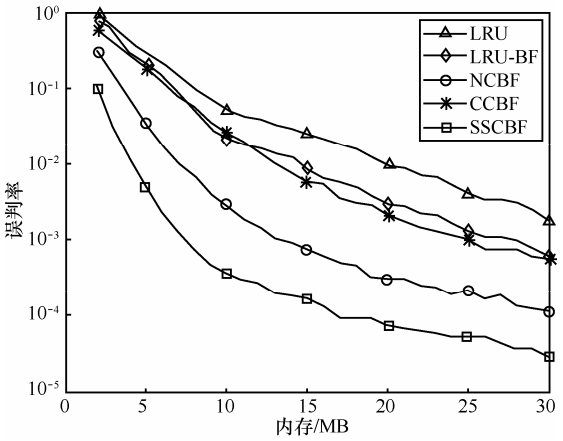


图 14　SSCBF 算法与其他算法的比较

从图 14 也可以看出，同样误判率条件下，SSCBF 比 NCBF 和 CCBF 算法所需内存空间都少，当误判率为 1%时，SSCBF、NCBF 和 CCBF 对应的内存占用分别为 4 MB、6 MB 和 13 MB。在同样误判率指标下，SSCBF 与 NCBF 相比，其内存占用减少约 33%。

7　时间复杂度分析与实验

7.1　时间复杂度分析

基于布鲁姆过滤器设计的抽样算法计算时间可以分为以下几部分。

T_h：计算 k 个散列值的消耗时间。

T_q：判断 k 个计数器向量是否超过阈值消耗时间。

T_i：修改 k 个计数器向量消耗时间。

报文到达时，NCBF 算法需要计算 k 个散列值并判断流是否为已抽样流，如果是则直接结束，否则需要修改计数器向量。因此 NCBF 算法对每个接

收报文的平均处理时间为

$$T_{\mathrm{NCBF}} = T_h + T_q + \frac{n_2}{n} T_i \tag{14}$$

其中，n_2 为正在进行抽样的流数量，n 为存在的并发流数量。

报文到达时，SSCBF 同样需要计算 k 个散列值并判断流是否为已抽样流，SSCBF 算法对每个接收报文的平均处理时间满足

$$\begin{aligned} T_{\mathrm{SSCBF}} &= T_h + T_q + \frac{n_2}{n}\left(T_q + T_i + \frac{n_3}{n} T_i \right) \\ &< T_h + T_q + \frac{n_2}{n}(T_q + 2T_i) \end{aligned} \tag{15}$$

其中，n_3 为抽样正好结束的流的数量。

因此对一个报文，SSCBF 算法比 NCBF 平均增加的时间不高于

$$T_{\mathrm{SSCBF}} - T_{\mathrm{NCBF}} = \frac{n_2}{n}(T_q + T_i) \tag{16}$$

考虑到 n_2 远小于 n，并且 T_q+T_i 远小于计算复杂度更高的 T_h，因此 SSCBF 算法增加的时间可以忽略不计。

7.2　算法处理速度实验

本节实验均使用 3.1 节进行抽样结束比率分析实验时的 New Zealand ISP 数据集，实验计算机配置与 5.3 节实验用计算机配置相同。为了降低磁盘 IO 对算法处理时间的影响，将数据集文件预先读入内存，然后基于抽样算法进行检测。散列函数数目分别选择 1~7，分别计算算法每秒能够处理的报文数目。为了减少操作系统突发任务对算法处理的干扰，重复进行 10 次实验，根据平均值得出算法的最终报文处理速度如表 2 所示。结果表明 SSCBF 算法的分组处理速度与 NCBF 的处理速度相比略有下降，与 6.1 节的分析基本吻合。另外，与 LRU 算法相比，随着散列函数数目增加，算法分组处理速度下降较快，当散列函数个数 k>2 时，SSCBF 分组处理速度会低于 LRU。这是因为仿真实验时散列函数计算量较大，并且采用串行处理方式进行，消耗了大量 CPU 处理资源。在实际系统设计时，可以采用并行处理的硬件来实现散列函数，提高处理速度。

8　结束语

在线流量识别为了提高识别速度，通常只采用流建立初期的若干数据分组进行分析。本文首次提出早期流量抽样技术，研究高速网络中如何获取流建立初期的数据分组。本文设计了同源组合布鲁姆过滤器 SSCBF 结构，结构中包括流抽样向量 sample 和分组计数向量 packet，2 个向量宽度不同，采用相同的散列源函数计算散列位置。基于 SSCBF 结构设计的早期流量抽样算法利用 2 个计数器向量分离了流抽样判断与分组计数检测，避免了大量抽样已经结束的流对分组计数过程的影响。算法误判概率、时间复杂度和空间复杂度等方面的分析和验证结果表明：在相同内存资源限制下的条件下，SSCBF 的误判率远低于同类算法；在同样误判率指标下，SSCBF 与其他算法相比，其内存占用至少减少 33%；在算法的处理速度方面，与 NCBF 相比，SSCBF 中的 2 个计数器向量均采用相同的散列源函数，增加的计算开销很小；随着散列函数数量的增加，算法的处理速度略低于 LRU 算法，在实际系统设计时，可以采用硬件实现算法中的散列函数，以提高处理速度。

参考文献：

[1] BERNAILLE L, TEIXEIRA R, AKODKENOU I. Traffic classification on the fly[A]. ACM SIGCOMM Computer Communication Review[C]. 2006, 36(2): 23-26.

[2] 杨哲, 李领治, 纪其进. 基于最短划分距离的网络流量决策树分类方法[J]. 通信学报, 2012,33(3):90-102.
YANG Z, LI L Z, JI Q J. Algorithm based on double counter bloom

表 2　　**不同散列函数时算法处理速度**

算法/(Mpacket·s^{-1})	k=1	k=2	k=3	k=4	k=5	k=6	k=7
NCBF	5.825	3.883	2.504	2.084	1.780	1.542	1.393
SSCBF	5.821	3.878	2.501	2.080	1.775	1.539	1.390
LRU-BF	5.412	3.551	2.294	1.975	1.710	1.505	1.366
LRU	4.218	4.218	4.218	4.218	4.218	4.218	4.218

filter for large flows identification[J]. Journal on Communications, 2012,33(3):90-102

[3] 张宏莉, 鲁刚. 分类不平衡协议流的机器学习算法评估与比较[J]. 软件学报, 2012, 23(6):1500-1516.
ZHANG H L, LU G. Machine learning algorithms for classifying the imbalanced protocol flows: evaluation and comparison[J] . Journal of Software, 2012, 23(6):1500-1516

[4] Cisco. Random sampled netflow[EB/OL]. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a7618.html

[5] ABHISHEK K, JUN X. Sketch guided sampling-using on-line estimates of flow size for adaptive data collection[A]. Proceedings of IEEE INFOCOM[C].2005.432-445

[6] 王洪波, 裴育杰, 林宇等. 基于 LRU 的大流检测算法[J]. 电子与信息学报, 2007, 29(10):2487-2492.
WANG H B, PEI Y J, LIN Y, *et al*. A LRU based algorithm for identifying and measuring large flow[J]. Journal of Electronics & Information Technology, 2007, 29(10): 2487-2492.

[7] 张震, 汪斌强, 张风雨. 基于 LRU-BF 策略的网络流量测量算法[J]. 通信学报, 2013,(1): 111-120.
ZHANG Z, WANG B Q, ZHANG F Y. Traffic measurement algorithm based on least recent used and Bloom filter[J]. Journal on Communications, 2013, (1): 111-120

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

[9] 吴桦, 龚俭, 杨望. 一种基于双重 Counter Bloom Filter 的长流识别算法[J].软件学报, 2010,21(5):1115-1126.
WU H, GONG J, YANG W. Algorithm based on double counter bloom filter for large flows identification[J]. Journal of Software, 2010, 21(5): 1115-1126.

[10] FAN L, CAO P, ALMEIDA J. Summary cache: a scalable wide-area web cache sharing protocol[J]. IEEE/ACM Trans on Networking, 2000, 8(3):281-293.

[11] SAAR C, YOSSI M. Spectral Bloom filters[A]. Proceedings of ACM SIGMOD International Conference on Management of Data[C]. San Diego, California, USA, 2003.241-252.

[12] FLAVIO B, MICHAEL M, RINA P, *et al* An improved construction for counting Bloom filters[A]. Proceedings of the 14th Conference on Annual European Symposium[C]. Zurich, Germany, 2006.684-695.

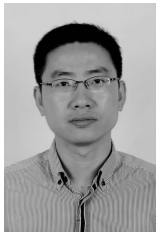
[13] NLANR. National laboratory for applied network research[EB/OL]. http://pma.nlanr.net/.

[14] 谢鲲, 文吉刚, 张大方等. 布鲁姆过滤器查询算法[J].软件学报, 2009, 20(1): 96-108.
XIE K, WEN J G, ZHANG D F, *et al*. Bloom filter query algorithm[J].Journal of Software,2009,20(1):96-108.

作者简介：

侯颖（1973-），女，河北唐山人，国家数字交换系统工程技术研究中心副研究员，主要研究方向为网络信息安全。

郭云飞（1963-），男，河南郑州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为新型网络体系结构、移动互联网。



黄海（1975-），男，江西南昌人，国家数字交换系统工程技术研究中心副教授，主要研究方向为通信与信息处理和网络信息安全。

王凯（1980-），男，河南许昌人，国家数字交换系统工程技术研究中心博士生，主要研究方向为网络信息安全和并行处理。