基于多维计数型布鲁姆过滤器的大流检测机制

张 震 汪斌强 陈庶樵 朱 珂
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：高速网络环境中，实时、准确地提取大流量对于网络安全和网络管理具有重要意义。该文针对传统的流量测量方法受计算资源和存储资源的限制，提出了一种基于多维计数型布鲁姆过滤器(Multi-Dimensional Counting Bloom Fliter, MDCBF)的大流检测机制。它将 1 维的计数型布鲁姆过滤器(Counting Bloom Fliter, CBF)结构，扩展到支持多维业务流表示、查询和统计计数的 MDCBF 结构。基于“Apriori 原理”，通过对 MDCBF 实施重正化，实现了用户自定义的大流检测。并能自适应地配置 CBF 参数，允许测量误差控制在预定义的范围内。基于计算机产生的模拟数据和实际互联网数据进行了仿真实验，结果显示：该方法既能获得较小的测量误差，又能获得较高的空间利用率。

关键词：网络测量；流量测量；布鲁姆过滤器；Apriori 原理；大流检测
中图分类号：TP393.06 **文献标识码**： A **文章编号**：1009-5896(2010)07-1608-06
DOI: 10.3724/SP.J.1146.2008.01699

A Mechanism of Identifying Heavy Hitters Based on Multi-dimensional Counting Bloom Filter

Zhang Zhen Wang Bin-qiang Chen Shu-qiao Zhu Ke
(*National Digital Switching System Engineering & Technological R & D Center*, *Zhengzhou* 450002, *China*)

Abstract: In high-speed network, identifying heavy hitters precisely in time serves as great significance for both network security and network management. In order to circumvent the deficiency of the limitted computing and storage abilities in traditional traffic measurement, a novel mechanism called identifying heavy hitters based on Multi-Dimensional Counting Bloom Filter(MDCBF) is proposed. Extending the standard structure of Counting Bloom Filter(CBF) to multi-dimensional one, the mechanism can not only represent, query and count traffic flows, but also sustain real time multi-granularity measurement. Based on Apriori principle, it can realize the identification of heavy hitters through implementing renormalization of MDCBF. Experiments are conducted based on the data either randomly produced by computer or sampled from the real network trace. Results demonstrate that the proposed mechanism can achieve finer space saving without sacrificing accuracy.

Key words: Network measurement; Traffic measurement; Bloom Filter; Apriori principle; Identifying heavy hitters

1 引言

高速网络中的流量测量是网络行为和流量工程技术研究和发展的重要依托，通过对流量的测量和分析可以把握网络行为的基本特征，有助于寻找网络行为的变化规律，构造并验证网络行为的数学模型。但是，随着网络技术的不断发展，特别是 Gbit 和 Tbit 网络技术的出现，导致链路带宽快速增长和网络流量急剧膨胀，网络测量面临着可扩展性的挑战：一方面，网络中的流数量每小时已经超过百万，而目前半导体工业不能提供维护每流状态所需的大量高速存储器；另一方面，访问和更新保存流量信息的存储器(DRAM)的速度(每年增长 7-9%)和网络链路的速率(每年增长 100%)之间的差距越来越大[1]。

为了适应高速网络的发展，Cisco 路由器提供了 NetFlow[2]产品来测量 IP 流，并引入了抽样测量技术，即在路由器内存中维护抽样报文的流记录。但是，由于网络流量的实时变化特性，抽样测量机制的准确度完全依赖于大流的检测率，一个或者几个大流的丢失就会影响整个流量测量的准确性。基于 Hash 算法的流量测量方法，是另外一种可扩展的测量机制：Bloom Filter(一种特殊的基于哈希算法的数据结构)能快速地鉴别 IP 流的信息，并能把 TCP 流的信息维护从 96 bit 的五元组映射到很短的哈希

2008-12-15 收到，2010-04-26 改回
国家 863 计划项目(2007AA01z2a1)和国家 973 规划项目(2007CB307102)资助课题
通信作者：张震 zhangzhenhigh@gmail.com

串所代表的空间，极大地减少了由于维护五元组信息而带来的资源开销。

文献[3]提出了一种基于 Loop Bloom Filter 的业务流计数的方法，并且引入了“time out”机制，但是该方法只能进行粗粒度的计算(只能计算并发业务流的总数，不能进行每流计数)，并且“time out”机制操作复杂，不具有可扩展性。文献[4]基于 Bloom Fliter 的数据结构提出了一种 IP 流的抽样方法，该方法具有 10 G 处理能力和较小的空间复杂度。文献[5]使用带哈希增强算法的 Bloom Filter Reproduction 方法对 TCP 连接大规模异常的参数进行快速再现，使得在检测过程中无须维护 TCP 五元组的信息。本文提出的大流检测机制主要采用了以下方法：将 1 维的 CBF 结构扩展到能够支持多维业务流统计和测量的 MDCBF 结构；基于“Apriori 原理”，重正化 CBF 中低于某一阈值的计数器单元，进而删除一些流量较小的 IP 流；自适应地配置 CBF 参数，允许测量误差控制在预定义的范围内。

2　SBF，CBF 和 MDCBF 结构描述

标准布鲁姆过滤器(Standard Bloom Filter, SBF)的核心是一个 $\boldsymbol{V}$ 向量和一组 Hash 函数，其原理如图 1 所示。设集合 $S=\{s_1,s_2,\cdots,s_n\}$ 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 $\boldsymbol{V}$ 中。每一个 Hash 函数相互独立且函数的取值范围为 $\{0,1,2,\cdots,m-1\}$。集合到向量 $\boldsymbol{V}$ 的映射过程如下：将向量 $\boldsymbol{V}$ 所有比特位置初始化为 0；当元素 s_i 插入集合 S 时，计算 $h_j(s_i)(1\le j\le k)$，若 $h_j(s_i)=q$，则令 BF[q]=1，将向量对应位置置位；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 $\boldsymbol{V}$ 的 k 个位置 $(h_1(x),h_2(x),\cdots,h_k(x))$ 是否为 1，如果其中有一个为 0，则 $x\notin S$；若全部值为 1，则 x 可能属于 S 中。由于存在哈希冲突，可能出现将不属于集合的元素误判成属于集合的“假阳性误判”，但不会出现将属于集合的元素误判成不属于集合的“假阴性误判”，SBF 的“假阳性误判率”(要求 k 个 Hash 函数都不遇见 0)为[6]

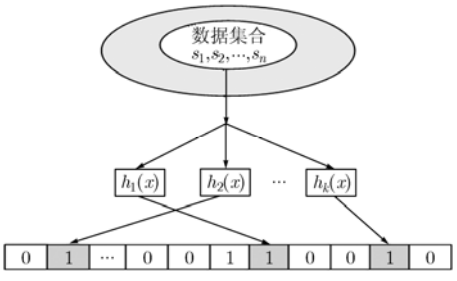

图 1 SBF 结构示意图

$$f^{\mathrm{BF}}(n,m,k)=(1-p)^k=\left(1-e^{-kn/m}\right)^k \tag{1}$$

SBF 能够较好地支持集合元素的插入和散列查询，但是不能够支持元素的删除。计数型布鲁姆过滤器可以解决这一问题：将向量 $\boldsymbol{V}$ 的每一维 $i(i\in\{1,2,\cdots m\})$ 设置成一个计数器，初值为 0。当要增加集合元素 x 时，令 $c(h_j(x))=c(h_j(x))+1$，(j=1,2,…,k)；当要删除集合元素 x 时，令 $c(h_j(x))=c(h_j(x))-1$，(j=1,2,…,k)。文献[6]证明了：当一组无重复的元素插入到一个 CBF 中时，CBF 中计数器单元的大小为 16(即每计数器 4 bit)就可以基本保证计数器不会因累加而溢出，其溢出概率满足 $P(\max(c(i))\ge 16)\le 1.37\times10^{-15}m$。

如图 2 所示，为了达到统计计数的目的，可以扩展 CBF 的功能：当 s_i 插入以后(设 s_i 对应的计数器为 $c(1),c(2),\cdots,c(k)$)，若后面到达的数据中还存在 s_i，则 CBF 不只是判断 s_i 存在，而且还应该在对应的计数器位置加 1 计数，统计 s_i 的个数。在不考虑计数器溢出的情况下，s_i 的统计值可以用 $\min\{c(1),c(2),\cdots,c(k)\}$ 来表示[7]，但存在单边“假阳性”的错误概率(即统计值比实际值大)。根据式(1)，布鲁姆过滤器的误判概率只和 (n,m,k) 有关，与每个计数器的大小无关。所以，CBF 的“假阳性”错误概率和 SBF 相等，即

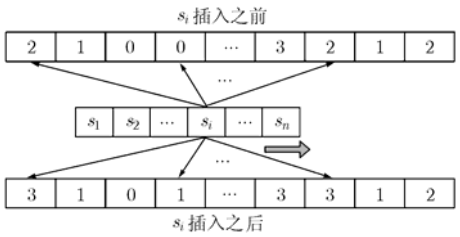

图 2 CBF 结构示意图

$$f^{\mathrm{CBF}}(n,m,k)=f^{\mathrm{SBF}}(n,m,k)=(1-p)^k=(1-e^{-kn/m})^k \tag{2}$$

SBF 和 CBF 的研究主要集中在单维元素的表示和查询，如：分档布鲁姆过滤器算法[8]和可扩展的布鲁姆过滤器算法[9]。结合流量测量的实际需要，即每个业务流都有五元组唯一标识，特引进高效的、空间简洁的多维计数型布鲁姆过滤器。为了对多维属性的流进行表示、查询和统计，MDCBF 采用和业务流维数相同的多个 CBF 组成，直接将业务流的表示和查询分解为单属性子集合的表示查询，业务流的维数有多少，就采用多少个 CBF 进行对应表示。一般用 $\{n,m,k,l\}$ 来表示 MDCBF，其中 l 表示业务流的维数。判断元素是否从属于集合，需要判断

业务流的所有属性字段是否在对应的属性子集合中。类似于 SBF 和 CBF，易得 MDCBF 的单边错误概率为

$$f^{\mathrm{MCBF}}(n,m,k,l)=\prod_{i=1}^{l}f^{\mathrm{CBF}}(n,m,k,l)=\left(f^{\mathrm{CBF}}(n,m,k)\right)^{l} \tag{3}$$

3 基于“Apriori 原理”的 MDCBF 大流检测机制

3.1 Apriori 原理

在 MDCBF 的架构下，特引进“Apriori”原理进行大流检测。为方便描述，特做出如下定义：

定义 1 标识业务流的每维属性字段，称作项，如源 IP 地址、源端口等字段。

定义 2 若只用一项来标识某一业务流，且此流的大小(以每流报文数来衡量)大于给定的阈值 M，那么标识该流的项称为频繁项。

定义 3 由 l 个项共同标识的某业务流，称为 l-项流；若 l-项流的大小大于给定的阈值 M，称此流为 l-项大流。

由以上定义可以看出：标识业务流的每一项，都有相应的 CBF 与之对应，即 l-项流要用 l 个 CBF 来联合表示、查询和统计。下面给出“Apriori 原理”的详细描述。

定理 1 Apriori 原理 1 如果一个流是 l -项大流，则它的所有子集一定是频繁的。

为了解释先验原理 1 的基本思想，假定某一个业务流用$\{A_1,A_2,\cdots,A_l\}$来标识一个流 f，且该流是 l-项大流。并设定它的α项子集$(1\le\alpha\le l)$来标识的业务流为 f'。因为属于流f的报文，也必定属于流 f'，所以 f' 也是α-项大流。相反，如果一个α项子集是非频繁的，则它的所有超集也一定是非频繁的。特别当α=1时，即如果1项子集是(单维属性字段的流)非频繁的，则它的所有超集也一定是非频繁的。

定理 2 Apriori 原理 2 如某一项是频繁项，则该项对应的CBF中的k个计数器也一定是频繁的(每个计数器的值都大于 M)。

为了解释先验原理 2 的基本思想，假定标识某 1-项流 f的项(设其为 A_1)为频繁项，根据定义 2，1-项流 f 是大流。令频繁项 A_1 对应的 k 个计数器为 $c(1),c(2),\cdots,c(k)$。由 CBF 的原理可知，业务流 f 的大小可表示为 $\min\{c(1),c(2),\cdots,c(k)\}$。用反证法，假定其中某一计数器 $c(i)<M$(M 为预设的阈值)，则业务流 f的大小必然小于 M，与“f是大流”矛盾，故先验原理 2 是成立的。相反，如果 k 个计数器中有任意一个小于预设的阈值，则 k 个计数器所对应的项也一定是非频繁的。

3.2 MDCBF 的重正化

流量测量设备一般每隔固定的时间间隔输出流量测量结果[10]，并把该测量间隔分成更小的时间窗。为方便描述，特做如下定义：

定义 4 流量测量设备每隔一定的时间间隔输出流量结果，称此时间间隔为测量周期 T。

定义 5 测量周期分成的等长时间间隔(设其为 T_h)，称为时间窗(Time Window，TW)。

为了统计大流量对象，基于定理 1 和定理 2，在每个时间窗结束时，需要重正化 MDCBF。下面针对标识某 l-项流的其中一项 A_i(某维属性字段)来讨论，设表示和查询 A_i 的计数型布鲁姆过滤器为 CBF_i。在任意时间窗 TW_j结束时，CBF_i重正化过程设计为：设阈值为 M，则对于 $c(k)<M$ (k=1,2,3,$\cdots$,m)的计数器，令 $c(k)$=0。

如果某计数器的值重正化后变成了 0，则该计数器对应项的统计值也变成了 0，并且基于先验原理 1，由此项标识的 l-项流的统计值也变成了 0(即该流被剔除)。例如：假设 A_1(源 IP 地址，其具体的值为 192.168.199.27)和 A_2(目的 IP 地址，其具体的值为 192.168.199.33)共同标识的 2-项流为 f_1，令 A_1 项对应的 CBF 的 k 个计数器为 $c(1),c(2),\cdots,c(i),\cdots,c(k)$；如果经过重正化后 $c(i)$(由于 $c(i)<M$)变成了 0，则 A_1 项的统计值可表示为 $\min\{c(1),c(2),\cdots,0,\cdots,c(k)\}=0$；2-项流 f_1 的统计值为 $\min\{\mathrm{sizeof}(A_1),\mathrm{sizeof}(A_2)\}=\min\{0,\mathrm{sizeof}(A_2)\}=0$，即该 2-项流 f_1 在 MDCBF 中被删除。

基于“Apriori 原理”重正化 MDCBF，一方面，可以统计到大于某一阈值的业务流，即用户可以根据实际的网络环境设置相应的阈值，得到相对意义上的大流；另一方面，压缩了流量信息存储的空间。

3.3 预定义测量误差

由于基于 MDCBF 的流量测量机制只存在单边“假阳性”的测量误差，网络管理员可以能够根据实际情况，预先设定测量误差，并在测量过程中动态配置 CBF 的个数，控制流量测量的性能。为了能够支持“预定义测量误差”，令标识业务流的某项 A_i对应的计数型布鲁姆过滤器不再是单个 CBF，而是一个 CBF 向量为 $\mathbf{CBF}_i$。并假设其中的每一个 CBF 预定义的最大单边错误概率为 f_0。由式(2)可知，当单边错误概率为 f_0，对应的过滤器所能统计的业务流个数为：$n_0=-(\ln(1-e^{\ln f_0/k})\cdot m)/k$。若使单边错误概率满足：$f^{\mathrm{CBF}}(n,m,k)\le f_0$，则此 CBF 所能容纳的业务流的个数 n 满足：

$$n \le n_0 = -\left(\ln\left(1-e^{\ln f_0/k}\right)\cdot m\right)\Big/k \tag{4}$$

在进行实时流量测量过程中，当 CBF_i^0 统计的业务流的个数 $n \ge n_0$ 时，增加一个新的 CBF_i^1；然后，用 CBF_i^1 来 Hash 统计后面顺序到达的业务流；当 $n \ge 2n_0$ 时，再增加一个新的 CBF_i^2，依次类推。设在测量周期 T 内，在向量 $\mathbf{CBF}_i$ 中被统计的流有 L 个，则需要相应的 CBF 个数为 $\lfloor L/n_0 \rfloor+1$，即 $\mathbf{CBF}_i=\{\mathrm{CBF}_i^0,\mathrm{CBF}_i^1,\mathrm{CBF}_i^2,\cdots,\mathrm{CBF}_i^{\lfloor L/n_0\rfloor}\}$。

4　实时测量过程

4.1 添加业务流

MDCBF 添加业务流的过程如表 1 所示。首先确定该业务流是多维属性流，即为多项标识的业务流，每项对应一个 CBF 向量。CBF 向量形成过程如下：

表 1 MDCBF 业务流的添加过程

```
Algorithm 1 InsertFlow(Object Flow)
Input: An object flow with multi-attributes
Output: void
Int addr[k]
For(i=0; i<Flow. Attr_length; i++)//Flow. Attr_length 为业务流的项数(维数)
    CBF=GetCBF(i);//获得第 i 维属性对应的 CBF 过滤器向量
    Hash=GetHash(i);//获得 Hash 函数
    IF(CBF.n>CBF. n0)//CBF 的误判率超过 f0
        CBF. Extention_time++;//初值为 0，其值为增加的过滤器个数
        CBF[CBF. Extention_time]=NewCBF(i);//创建一个新的过滤器
        CBF. n0=CBF. n0+n0;//n0值为单个 CBF 所能容纳的最大业务流个数
    End if
    For(j=0; j<k; j++)
        addr[j]=Hashj[Flow. attr[i]];//计算第 i 维属性的 Hash 值
        CBF[CBF.Extention_time]. osition[addr[j]]++;//将 CBF[CBF. Extention_time]//中相应的位置 1 加计数
    End for
End for
```

步骤1　初始化各个参数。确定流f的项数l(如果用源IP地址和目的IP地址来共同标识一个流，则l=2；如果用五元组标识一个流，则l=5)；初始化l个CBF，令每个CBF中的计数器的值为0；确定k个Hash函数。

步骤2　提取属性字段A_i(即A_i项，存放在数组Flow.attr[Flow.attr_length]里面)，获得A_i对应的向量$\mathbf{CBF}_i$。

步骤3　判断向量$\mathbf{CBF}_i$的误判率是否超过预设测量误差(等价于判断CBF.n>CBF.n_0是否成立，其中CBF.n为向量$\mathbf{CBF}_i$当前存储A_i项的个数，CBF.n_0是向量$\mathbf{CBF}_i$允许存的最大数目)。若判断条件成立，则为$\mathbf{CBF}_i$增加一个新的CBF，以后每次到达的新业务流都Hash到这个新增的CBF中，然后执行步骤4；反之，直接执行步骤4。

步骤4　对A_i进行Hash运算，得到k个Hash地址$h_1(A_i),h_2(A_i),\cdots,h_k(A_i)$；找到对应的$k$个计数器$c(1)$=CBF$[h_1(A_i)]$，　$c(2)$=CBF$[h_2(A_i)]$，　$\cdots$　，$c(k)$=CBF$[h_k(A_i)]$；令$c(1)=c(1)+1$，$\cdots$，$c(k)=c(k)+1$。

步骤5　令 $i=i+1$，重复步骤 2、3、4，直到 $i=l$，即在向量 $\mathbf{CBF}_i$ 中添加完标识该业务流的所有 l 项。

4.2 业务流的统计过程

该流量测量机制主要包括以下几个部分：在单个时间窗口，基于 MDCBF 的业务流统计；时间窗结束时，重正化 MDCBF；测量周期结束时，强制输出测量结果，统计过程如表 2 所示。

表 2 MDCBF 的实时测量过程

```
Algorithm 3 MDCBF (Object Flow)
Input: An object flow with multi-attributes
Output: Measurement Results
Int T1= Th
If (t>T1)//判断时间窗 Th是否结束
    Renormalize(MDCBF);//重整化 MDCBF
    T1=T1+Th; //进入下一个时间窗
End if
InsertFlow(Object Flow); //统计业务流
If(t>T)//判断测量周期是否结束
    Return(MDCBF_Result);//输出测量结果
End if
```

一方面，由于统计业务流过程只需要一次 Hash 映射计数以及 Hash 函数的并行操作性，使得流量测量的计算复杂度大大降低；另一方面，使用 MDCBF 能把流信息维护从 96 bit 的五元组映射到很短的哈希串所代表的空间，极大地减少了由于维护五元组信息而带来的资源开销，为业务流的实时统计提供了条件。

5　仿真实验

为了验证 MDCBF 大流检测机制的性能，本节采用两种实验方法：计算机随机产生的多维数据元素；对实际网络链路采集得到的数据进行统计分析。

在实验中针对不同维的数据进行了统计分析，以进一步体现该机制能够支持多维业务流的统计测量。

5.1 模拟流量数据仿真

通过随机实验验证算法的性能，对二维、三维、四维、五维的数据分别进行实验。实验步骤如下：

步骤 1 定义多维数据元素。每一维数据采用 16 bit 的整数，这些整数都是由计算机随机生成的无符号整数，数值范围[0，2^{16}–1]。如：l 维数据可以表示为：$\{d_1,d_2,d_3,\cdots,d_l\}$,其中 d_i 为 16 bit 的无符号整数。

步骤 2 确定 Hash 函数。实验中采用文献[6]中定义的 H_3 散列函数，H_3 散列函数具有很强的随机性，是一种常用的布鲁姆滤波器的实现函数。多维数据的每个属性可以通过 H_3 函数映射到对应 CBF 中的相应计数器位置。

步骤 3 产生多维数据元素。首先，用计算机随机产生 1000 个互不相同的元素 $S=\{s_1,s_2,\cdots,s_{1000}\}$；然后，每个元素重复产生，且每个元素重复产生的次数在{0,1,2,⋯,20}之间等概率选择，所以，要 Hash 统计的平均数据个数为 10000。

步骤 4 **MDCBF** 统计计数。初始化 M=5，k=7，n_0=500, m=32768，即每一维数据需要 2 个 CBF 即可；基于 MDCBD 进行统计计数。

步骤 5 测量结果分析。如果某元素的统计值大于其实际值，则认为这是一次“假阳性”错误，实际错误概率定义为：发生假阳性错误概率的元素个数/数据元素的总数 1000。仿真比较错误概率的理论值和实际值;计算 MDCBF 所需要的空间大小。

通过表 3 和表 4 可以看出：在不考虑计数器“溢出”的情况下，仿真实验的错误概率和理论值十分一致，并且仿真实验的标准差比较小，验证了式(3)的正确性；使用相同的 Hash 函数的个数，数据的维数越大，统计的错误概率越小；当 L=2,3,4,5 时，空间利用率分别为 33 bit/元素，50 bit/元素，65 bit/元素，80 bit/元素，其空间消耗比较少，具有布鲁姆过滤器节约空间的特性。

表 3 2 维和 3 维数据的错误概率仿真

Hash 函数	2 维			3 维		
	k=4	k=6	k=8	k=4	k=6	k=8
理论值	0.0821	0.1229	0.2236	0.0152	0.0431	0.1265
实验均值	0.0804	0.1236	0.2330	0.0148	0.0433	0.1214
实验标准差	0.0020	0.0030	0.0051	0.0012	0.0019	0.0041
空间大小(bit)		32768			49152	

表 4 4 维和 5 维数据的错误概率仿真

Hash 函数	4 维			5 维		
	k=4	k=6	k=8	k=4	k=6	k=8
理论值	0.0035	0.0151	0.0542	0.0008	0.0053	0.0241
实验均值	0.0031	0.0152	0.0542	0.0008	0.0053	0.0265
实验标准差	0.0003	0.0016	0.0020	0.0003	0.0007	0.0013
空间大小(bit)		65536			80240	

5.2 真实流量数据仿真

为了进一步验证 MDCBF 流量测量机制的有效性，实验 2 利用实际的网络链路数据进行统计分析，实验数据源来自 NLANR 的 OC-12 Trace[11]，持续时间为 100 s。为了体现该机制能够支持多维业务流的统计测量，主要对 2-项流(源 IP 地址、目的 IP 地址共同标识一个流)和 5-项流(源 IP 地址、目的 IP 地址、目的端口、源端口和协议字段共同标识一个流)进行统计测量。实验中，流的大小主要用每流报文数来衡量，设置 M = 100，k=7，n_0=1000, m=65536，T=100 s，T_h=1 s。

图 3 是业务流数量的实时统计图。横轴为业务流的持续时间，时间粒度为 1 s；纵轴为实时的业务流的数量。可以看出：MDCBF 能支持多粒度流量测量，并且 5-项流的统计个数要比 2-项流的统计个数多。这主要是因为 5-项流比 2-项流的区分粒度细，每秒钟统计的业务流总数固然要多一些。

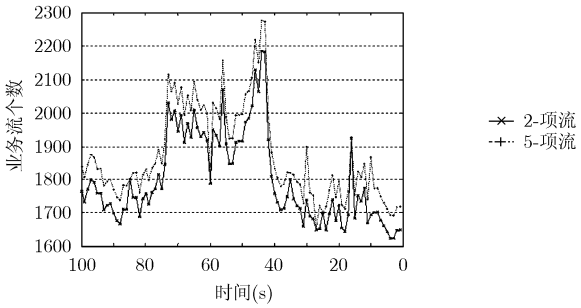

图 3 业务流的实时统计图

通过实际链路数据的处理，得到流量比重(按照业务流所拥有报文总数来衡量)占前 5 位的聚合业务流，如表 5 所示。根据表 5 可以得到如图 4 的误差曲线，其中错误概率为：发生假阳性错误概率的元素个数/数据元素的总数 1000。可以看出：使用相同的 Hash 函数的个数，被统计的业务流量越大，统计的错误概率越大，验证了式(1)–式(3)的正确性；在相同业务流量的情况下，Hash 函数越多，错误概

表 5 五种聚合业务流的流量百分比

聚合业务流	HTTP	P2P	FTP	SMTP	DNS
百分比(%)	53.21	20.67	7.64	3.45	1.50

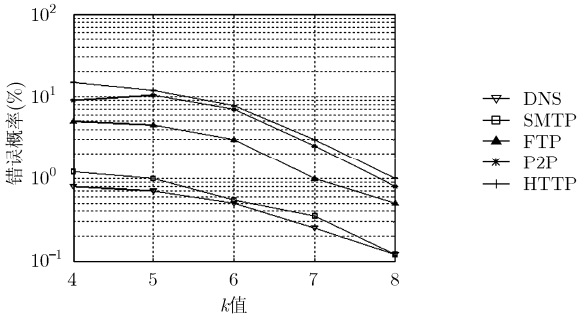

图 4 误差曲线图

率越小，也同时验证了式(1)-式(3)的正确性。

6 结束语

布鲁姆过滤器是一种简洁的数据表示结构，能支持大规模数据集合的表示和查询操作。本文基于 SBF 和 CBF 的相关理论，将布鲁姆滤波器由 1 维扩展到多维，构建了 MDCBF 的数据表示、查询和统计计数结构。将 MDCBF 结构引入到流量测量领域，一方面能支持多维业务流信息的统计测量；另一方面，基于“Apriori”原理，通过重正化 MDCBF，可以统计用户自定义的大流；再者，该流量测量机制还支持动态配置 CBF，把测量误差控制在预定义的范围内。仿真实验表明：基于 MDCBF 的流量测量机制在测量误差较小，能够获得较好的空间利用率，为高速网络流量的实时测量提供了条件。基于 MDCBF 的各种网络应用和如何设计一种扩展性更好的布鲁姆过滤器结构，将是本文下一步的研究方向。

参 考 文 献

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

[2] Cisco Netflow. http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml. 2008.

[3] Sun Yong, Zhang Zhi-bin, Guo Li, Bai Shuo, and Tan Jian-long. An effective algorithm for counting active flows based on loop filter[C]. Proc. International Conference on Networking, Architecture, and Storage, IEEE Computer Society, Chongqing China, 2008: 104−109.

[4] 王洪波, 程时端, 林宇. 高速网络超链接主机检测中的流抽样算法研究[J]. 电子学报, 2008, 36(4): 809−818.
Wang H B, Cheng S D, and Lin Y. On flow sampling for identifying super-connection hosts in high speed networks[J]. *Acta Electronica Sinica*, 2008, 36(4): 809−818.

[5] 龚俭, 彭艳兵, 杨望, 刘卫江. 基于 Bloom Filter 的大规模异常 TCP 连接参数再现方法[J]. 软件学报, 2006, 17(3): 434−444.
Gong J, Peng Y B, Yang W, and Liu W J. Reconstructing the parameter for massive abnormal TCP connection with Bloom filter[J]. *Journal of Software*, 2006, 17(3): 434−444.

[6] Fan Li, Cao P, Almeida J, and Broder A. Summary cache : A scalable wide−area web cache sharing protocol[J]. *IEEE/ACM Transactions on Networking*, 2000, 8(3): 281−293.

[7] Saar Cohen and Yossi Matias. Spectral Bloom Filters[C]. Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, San Diego. California, 2003: 241−252.

[8] 谢鲲, 闵应骅, 张大方, 谢高岗, 文吉刚. 分档布鲁姆过滤器的查询算法[J]. 计算机学报, 2007, 4(30): 597−607.
Xie K, Min Y H, Zhang D F, Xie G G, and Wen J G. Basket Bloom filter for membership queries[J]. *Chinese Journal of Computers*, 2007, 4(30): 597−607.

[9] Xie K, Min Y H, and Zhang D F, *et al*.. A Scalable Bloom filter for membership queries[C]. Proc of IEEE Globlecom. Washington D.C. USA, 2007: 543−547.

[10] Estan C, Keys K, Moore D, and Varghese G. Building a Better Netflow[C]. Proc. SIGCOMM'04, Portland, ACM Press, 2004: 245−256.

[11] NLANR. Inder of/Traces/Traces/daily/20050801. http://pma.nlanr.net/Traces/Traces/daily/20050801, 2008.

张　震：　男，1985 年生，博士生，研究方向为宽带信息网络、网络测量.

汪斌强：　男，1963 年生，教授，博士生导师，研究方向为宽带信息网络与高速路由器核心技术.

陈庶樵：　男，1973 年生，博士，副教授，研究方向为宽带信息网络与高速路由器核心技术.

朱　珂：　男，1975 年生，博士，讲师，研究方向为网络体系结构.