doi:10.3969/j.issn.1671-637X.2015.04.010

基于多位域的等概率随机IP流抽样算法

张毅卜[1]， 李 鑫[2]， 戢 勇[2]， 夏靖波[1]， 刘一博[1]
(1.空军工程大学信息与导航学院,西安 710077； 2.空军通信网络技术管理中心,北京 100843)

摘 要：对IP流信息的全方位提取有助于实现网络实时监控,精细管理,有利于网络安全性能的提升。已有的等概率随机IP流抽样算法将大量的IP流重复抽样,浪费了宝贵的计算和存储资源。针对这个问题,在原有算法的基础上设计了一种新的等概率随机IP流抽样算法,该算法在Bloom Filter的基础上采用三层位域,两层同时测量,结果取交集的方法,便于实际使用并且有效减少了已被抽样的IP流被重复抽样。实验结果表明:新方法能够大幅度提高测量精度,节约了系统资源,可以适用于10 Gb/s左右的高速网络之中。

关键词：高速网络； IP流； Bloom Filter； 等概率随机抽样； 装载因子
中图分类号：V271.4； TP393 **文献标志码**：A **文章编号**：1671-637X(2015)04-0046-04

An Equal Probability Random Sampling Algorithm of IP Flow Based on Multiple Bit Fields

ZHANG Yi-bo[1], LI Xin[2], JI Yong[2], XIA Jing-bo[1], LIU Yi-bo[1]
(1. School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China;
2. Air Force Communication Networks Technology Management Center, Beijing 100843, China)

Abstract: The omnidirectional collection of IP flow information is helpful for the real-time monitoring and precise management of the network, and also beneficial for improving the network security. The original IP flow sampling algorithm makes repeated sampling to the IP flow, resulting in a waste of storage and computing resource. Based on the original algorithm, a new method of IP flow sampling in high speed network with equal probability random is presented. This algorithm adopts three-level bit fields based on Bloom Filter, with two of them measured simultaneously for obtaining the intersection of their results. It is convenient and can prevent repeat sampling to IP flow effectively. The experimental results indicate that: The new algorithm can improve the measure precision drastically and make full use of the system resources, which is applicable to 10 Gb/s high speed network.

Key words: high speed network; IP flow; Bloom Filter; equal probability random sampling; fill factor

0 引言

当下网络流量的测量主要分为数据报文测量和IP流测量。IP流测量将具有相同属性的数据报文聚类进行分析[1],所需存储空间小,能够更好地反映数据报文之间内在的关系,已成为网络流量测量和网络状态感知的热点方向之一。

现有的基于IP流的抽样方法中,大部分小流由于被抽中概率小而被忽略,导致大量流信息丢失,这对于网络安全监测、网络异常检测等应用构成了隐患[2],因此有必要对IP流"公平"抽样展开研究。

在IP流"公平"抽样方面,SGS算法[3](Sketch Guided Sampling)通过设置包抽样比为所属流当前流量的递减函数,减少对大流数据包的抽样,增加小流数据包的抽样,更好地保证了数据包之间的抽样公平性。文献[4]提出了一种基于多解析度抽样统计器的数据包公平抽样算法(Space-Efficient Fair Sampling,SEFS),该算法可以很好地对各数据流的流量进行估计,有效地减少了测量中产生的哈希冲突。文献[5]在Bloom Filter的基础上提出了一种等概率随机网络流抽样算法,用以实现网络流的"公平"抽样,相比于前两种方法,该方法结构简单,易于硬件实现,便于大规模部署,但该算法在位域进行初始化时会把大量已识别的IP流重新认定为新流,造成重复抽样,测量时存在较大误差。

收稿日期:2014-05-16 **修回日期**:2014-06-23
基金项目:陕西省自然科学基金(2012JZ8005)
作者简介:张毅卜(1989—),男,陕西西安人,硕士生,研究方向为网络流量测量。

本文在文献[5]的基础上提出了一种基于三层位域的 IP 流等概率随机抽样算法，文章首先介绍原算法的基本思想，指出其存在的不足之处，设计出新的抽样算法，最后验证所提新算法。

1　相关工作

1.1　原算法基本思想

原算法主要由 Bloom Filter、误差吸收和随机抽样 3 个模块实现。Bloom Filter 作为一种简单高效、便于查找的运算机制，主要功能是判断到来的网络流是否是新流；随机抽样模块的主要功能是以调整后的概率对 Bloom Filter 认定的新流进行随机抽样；由于 Bloom Filter 存在误差，部分新流不能被其判断出，误差吸收模块的功能是根据误差概率来调整随机抽样率，把 Bloom Filter 所引起的误差吸收到随机抽样模块中，从而满足“等概率随机抽样”的要求；流计数器用以对插入到 Bloom Filter 中的流进行计数。

1.2　原算法分析

由文献[6]知，Bloom Filter 的误正率为

$$p=[1-(1-1/m)^{kn}]^k\approx(1-e^{-kn/m})^k \qquad (1)$$

式中：m 为位域的大小；k 为哈希函数个数；n 为统计得到的 IP 流数量。当一个数据分组到达时，Bloom Filter 首先计算其流 ID 的 k 个哈希函数值，这里 $k=3$，若位域 v 中的 k 个相应位均为 1，则认为没有新流到达，算法结束并继续处理下一个分组；反之，说明到达的流为新流，把该流插入到 Bloom Filter 中（把 k 个相应位置 1），然后根据此分组到达前 Bloom Filter 中已插入的流个数按照式(1)计算出误差概率 P，因此，一个新流被 Bloom Filter 成功检测出的概率为 $1-P$。当 Bloom Filter 发现一个新流时，如果调整随机抽样模块的抽样概率为 $r/(1-p)$（r 为整个算法的抽样概率），则可以保证任何一个新流被抽样的概率都等于 r（即 $(1-p)\times r/(1-p)$），从而满足了“等概率随机抽样”的要求。

与此同时，在位域中设定装载因子上限 $B_{max}=0.6$，当流计数器中记录的流个数 $n\geqslant(m/k)\times B_{max}$ 时，Bloom Filter 使用另外一个空的位域并开始新的测量周期，同时对暂不使用的位域进行初始化，两个位域交替使用以保持测量的连续。

文献[5]所提算法的重点在于如何在进行流识别时精确而有效地识别出新流并计算其数量。该算法充分利用了 Bloom Filter 简单高效、便于查找的特点，并且在随后的随机抽样模块中有效地“吸收”了 Bloom Filter 产生的误差，从原理上很好地实现了网络流的等概率随机提取，但是该算法在第一层位域进行初始化，使用第二层位域开始测量时，由于第二层位域为空，会把第一层位域中已识别的流再次认定为新流，并且在随后的计数器中重复计数，随机抽样模块随之再次进行抽样，在实际使用时存在较大误差。本文的主要工作正是对原算法 Bloom Filter 模块的改进。

2　算法改进

本文所提 TBF（Three-Bit-Field）算法在原算法两层位域的基础上再加入一层位域，并且为每个位域设置不同的装载因子，形成一个三层位域的测量架构，同时保持误差吸收模块和随机抽样模块架构不变。

将 3 个位域分别命名为 A_1，A_2，A_3，对应的装载因子上限分别为 B_1，B_2，B_3，哈希函数仍然使用 H_3 哈希函数。算法结构如图 1 所示。

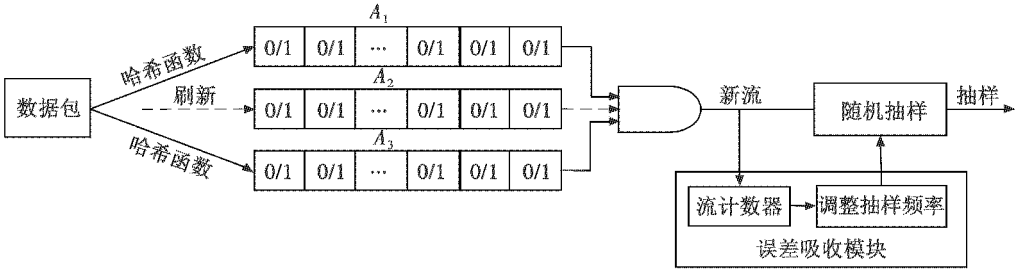

图 1　TBF 算法结构

Fig. 1　Structure of TBF algorithm

测量开始时，首先使用 A_1 和 A_2 位域进行测量，当一个数据包到来时，Bloom Filter 将数据包流关键字分别映射到两层位域之上，然后对两层位域分别得出的判定结果取交集，若两层位域所得结果均为真（即两层位域的 k 个相应位均存在 0），则认为到来的 IP 流为新流，将相应位分别置 1，同时流计数器加 1，反之说明到来的 IP 流已存在，算法结束并继续处理下一个分组。

不同的装载因子使得位域之间的初始化时间不同，当 A_1 位域的装载数量达到上限时，随即进行初始化，A_2 和新位域 A_3 同时工作，仍然可以对到来的数据包是否属于新流进行准确的判定，减少了对已识别流的重复认定。最后调整随机抽样概率，实现对 IP 流的等概率随机抽样。TBF 算法的具体实现步骤为：

1）分组 p' 到达，提取其流关键字 f；

2）抽取三层位域中的前两层 A_1，A_2，使用哈希函数将流关键字 f 分别映射到两层位域；

3）If(A_1 判定为新流)

$n_1 = n_1 + 1$

else 处理下一个分组

End；

If(A_2 判定为新流)

$n_2 = n_2 + 1$

else 处理下一个分组

End；

If(两层位域均判定为新流)；

流数量 $n = n + 1$，继续处理下一分组

End；

If $(n_{i(i=1,2)} \geqslant (m/k) \times B_{i(i=1,2,3)})$，初始化相应位域，使用另外一个空位域 A_3 继续进行测量

以此类推……

End；

4）计算 Bloom Filter 误正率 p_{TBF}；

5）调整随机抽样概率为 $r/(1-p_{TBF})$。

3 理论分析

3.1 准确性分析

由式(1)知：$p \approx (1-e^{-kn/m})^k$，即 $p = e^{\ln(1-e^{-kn/m})^k} = e^{k\ln(1-e^{-kn/m})}$。令 $p' = k\ln(1-e^{-kn/m})$，当 p' 取最小值时，p 也为最小值，设 $p'' = e^{-kn/m}$，则

$$p' = -m/n(\ln p''\ln(1-p'')) \text{ 。} \tag{2}$$

由对称性可知，当 $p'' = 1/2$ 时，p' 取最小值，误正率最小。由于 p'' 为 k 个哈希函数把 n 个元素映射到 m 位的位域中时某位仍为 0 的概率，所以当 $p'' = 0$ 时，位域中 0 和 1 各占一半，因此当位域中保持一半的位置未被置位时，将会保持较低的误正率[7]。设定哈希函数个数 $k = 3$，在不发生任何哈希碰撞的状态下，装载因子上限 $B_i = kn/m = 0.5$ 将会是最理想的状态，但是由于哈希碰撞的存在，$kn/m < 0.5$。因此，在实际的使用中，从节约内存的角度考虑，可以酌情将 B_i 增大。

假定使用中的两层位域产生的误差分别为 p_i 和 p_j，在 TBF 算法中，由于对两层位域的判定结果取交集，TBF 算法误正率为

$$p_{TBF} = 1-(1-p_i)(1-p_j) \tag{3}$$

即

$$p_{TBF} = p_i + p_j - p_i p_j \text{ 。} \tag{4}$$

由于 $0 < p_i < 1$，因此 $p_j - p_i p_j > 0$，$p_{TBF} - p_i > 0$。所以 TBF 算法的误正率比只使用一层位域进行测量的原算法高，该误正率会在随后的随机抽样模块中被“吸收”掉，对结果影响有限。

使用 A_1、A_2 位域测量时，当 A_2 位域达到装载上限初始化时，A_1 位域尚未使用的部分为 $A_1B_1 - A_2B_2$（假定 $B_1 > B_2$），设 X 为位域单位空间内存储的流的数量，Y 为其中已认定的流的比例，所以在使用 A_3 位域测量到 A_1 位域初始化时将会有 $XY(A_1B_1 - A_2B_2)$ 个已认定的流不会被再次认定为新流，减少了流的重复认定，提高了测量精度，节约了系统资源。

3.2 可行性分析

TBF 算法中，Bloom Filter 的哈希函数的计算速度和位域的访问速度很大程度上决定了整个算法的最快处理速度。本文中采用 H_3 哈希函数，该函数在运算中仅使用“与”和“或”逻辑，逻辑结构简单，易于计算机运算，具有较好的随机性，运算速度可达纳秒级[8]。现有的 SRAM 的访问速度已达到 2 ns，因此，虽然 TBF 算法的时间复杂度较原算法有所提高，但总的时间数量级仍小于 32 ns，足以应用于 OC192 链路之上。

4 仿真实验与结果分析

4.1 仿真

实验使用数据来源于互联网数据分析合作组织[9]（CAIDA）在不同时间发布的流量数据，具体情况见表 1。本实验选取两组流量数据的前 10 万个数据包作为实验对象，将 3 个位域的长度均设置为 50 000 b。

表 1 背景流数据信息

Table 1 Information of traffic data

实验数据	持续时间/s	链路速率/(Gb·s^{-1})	分组数量
trace-1	300	2.5	17 758 098
trace-2	10	2.5	618 209

实验中采用五元组作为流标识[10]，将第 1 组装载因子上限分别设置为 $B_{11} = 0.6$，$B_{12} = 0.7$，$B_{13} = 0.6$；第 2 组装载因子上限设置为 $B_{21} = 0.6$，$B_{22} = 0.7$，$B_{23} = 0.5$。图 2 和图 3 为采用两组装载因子上限时分别对 trace-1 流量数据的仿真结果，为了进一步证明算法有效性，使用 trace-2 再次验证，图 4 和图 5 为采用两组装载因子上限分别对 trace-2 流量数据的仿真结果。

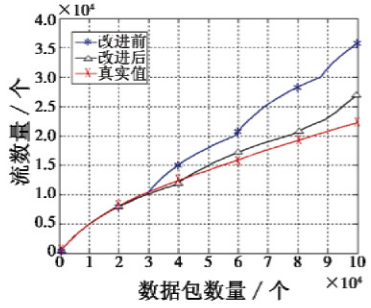

图 2 流数量比较图(trace-1，第 1 组装载因子)

Fig.2 Comparison of flow number(trace-1, the lst loading factor)

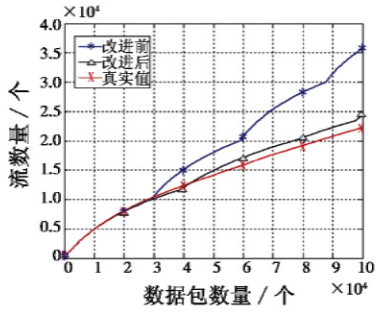

图 3　流数量比较图(trace-1,第 2 组装载因子)

Fig. 3　Comparison of flow number(trace-1,the 2nd loading factor)

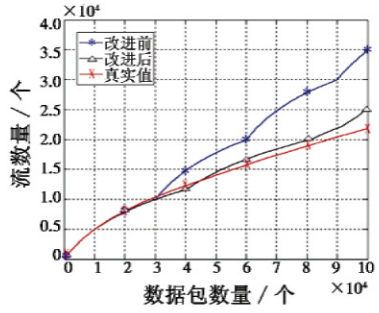

图 4　流数量比较图(trace-2,第 1 组装载因子)

Fig. 4　Comparison of flow number(trace-2,the 1st loading factor)

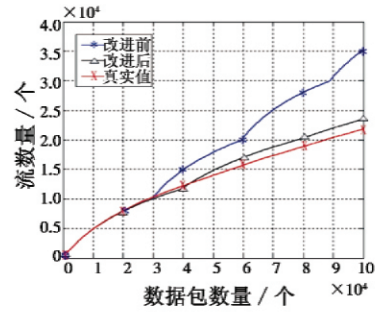

图 5　流数量比较图(trace-2,第 2 组装载因子)

Fig. 5　Comparison of flow number(trace-2,the 2nd loading factor)

通过对比仿真结果发现,原算法随着数据包的增多,所识别出的流数量逐渐脱离真实数量,误差较大;改进后的 TBF 算法减少了对已识别 IP 流的重复认定,所得结果更加趋近于真实值。

对比图 2 和图 3 可以看出,后者的结果更加趋近于真实值,这是因为装载因子上限 B_{23} 小于 B_{13},使用第 2 组装载因子上限测量时,未初始化的位域中保存着的流记录多于使用第 1 组,可以防止将更多已识别的流重新认定为新流,仿真结果更加精确。

由于 Bloom Filter 本身存在误正现象,因此在某些阶段会出现 TBF 算法统计值小于实际数量的情况,该部分误差产生的影响会在随后的随机抽样模块中被“吸收”掉,对最终结果影响有限。计算出流数量之后,随机抽样模块随之调整抽样概率为 $r/(1-p_{TBF})$,即可实现对 IP 流的等概率随机抽样。

4.2　误差分析

本文定义测量误差为 $\varepsilon = \bar{n} - n$,$n$ 为 IP 流数量真实值,$\bar{n}$ 为测量值,取每 10 000 个数据包为一个观测点。图 6 和图 7 分别为使用两组装载因子上限时 trace-1 流量数据所产生的误差。

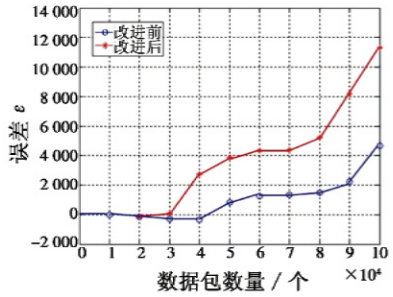

图 6　误差比较图(第 1 组装载因子)

Fig. 6　Comparison of error with the 1st loading factor

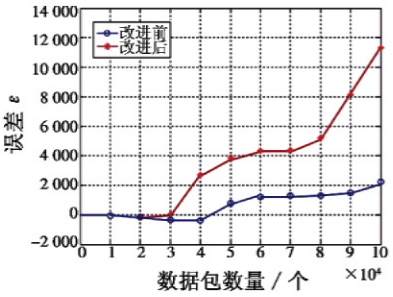

图 7　误差比较图(第 2 组装载因子)

Fig. 7　Comparison of error with the 2nd loading factor

可以看出,改进后的 TBF 算法有效地减少了对已认定 IP 流的再次认定,减小了测量误差,实验结果更加准确。

5　结束语

本文提出了一种基于三层位域的 IP 流等概率随机抽样算法,通过设置不同的装载因子上限,运用两层位域同时进行测量,对各位域测量结果取交集的方法得出最终结果。经过实验验证,该算法能够大幅度减小测量误差,提高网络流的识别精度,节约了系统资源,并且三层位域的交替使用使得该方法可以更好地进行工程应用。该算法在时间复杂度方面较原算法有所提高,下一步的研究应着重放在寻找随机性更佳、处理方式更加简便的哈希函数上。

参 考 文 献

[1]　钱宇. 高速网络流测量模型研究[D]. 郑州:解放军信息工程大学,2008. (QIAN Y. Research on high-speed network flow measurement model[D]. Zhengzhou: PLA Information Engineering University, 2008.)

(下转第 61 页)

[D]. Nanjing: Nanjing University of Science and Technology, 2008.)

[6] 吴瑕,周焰,崔建,等. 导弹防御系统中红外光电识别技术分析[J]. 红外与激光工程,2009,38(5):759-766. (WU X, ZHOU Y, CUI J, et al. Analyses on infrared optoelectronics recognition technology in missile defense system[J]. Infrared and Laser Engineering, 2009, 38(5): 759-766.)

[7] 赵延,姚康泽,孙俊华,等. 导弹预警卫星目标识别算法研究[J]. 系统工程与电子技术,2005,27(10):1811-1813. (ZHAO Y, YAO K Z, SUN J H, et al. Research on a new algorithm of missile target recognition of missile early warning satellite system[J]. Systems Engineering and Electronics, 2005, 27(10): 1811-1813.)

[8] 高山,王森,刘建华. 基于模板的天基预警系统目标性质匹配模型与仿真实现[J]. 空军工程大学学报:自然科学版,2011, 12(5):36-39. (GAO S, WANG S, LIU J H. Matching target character model and simulation realization of space ground warning system based on template [J]. Journal of Air Force Engineering University: Natural Science Edition, 2011, 12(5): 36-39.)

[9] 操乐林,武春风,侯晴宇,等. 基于光谱成像的目标识别技术综述[J]. 光学技术,2010, 36(1): 145-150. (CAO L L, WU C F, HOU Q Y, et al. Survey of target recognition technology based on spectrum imaging[J]. Optical Technique, 2010, 36(1): 145-150.)

[10] NEELE F. Two-colour infrared missile warning sensors [C]//Proceedings of SPIE, Airborne Intelligence, Surveillance, Reconnaissance (ISR) Systems and Applications II, 2005, 5787: 134-145.

[11] GOLDBERG A. Dual band infrared imagery of an Atlas 5 launch vehicle in flight[J]. AIAA, 2005, 43(1): 174-183.

[12] AMINOV B, ROTMAN S R. Spatial and temporal point tracking in real hyperspectral images[C]//IEEE 24th Convention of Electrial and Electronics Engineers in Israel, 2006: 16-20.

[13] 王润生,杨苏明,阎柏琨. 成像光谱矿物识别方法与识别模型评述[J]. 国土资源遥感,2007(1):1-9. (WANG R S, YANG S M, YAN B K. A review of mineral spectral identification methods and models with imaging spectrometer[J]. Remote Sensing for Land & Resources, 2007(1): 1-9.)

[14] 许毅平. 基于高光谱图像多特征分析的目标提取研究[D]. 武汉: 华中科技大学,2008. (XU Y P. Study on object extraction based on multi-feature from hyperspectral image[D]. Wuhan: Huazhong University of Science and Technology, 2008.)

(上接第 49 页)

[2] 杨家海,吴建平,安常青. 互联网络测量理论与应用[M]. 北京:人民邮电出版社,2009. (YANG J H, WU J P, AN C Q. The theory and application of internet measurement[M]. Beijing: Posts & Telecom Press, 2009.)

[3] KUMAR A, XU J. Sketch guided sampling—using on-line estimates of flow size for adaptive data collection[C]// The 25th IEEE International Conference on Computer Communications, 2006: 1-11.

[4] 张进,邬江兴,钮晓娜. 空间高效的数据包公平抽样算法[J]. 软件学报,2010,10:2642-2655. (ZHANG J, WU J X, NIU X N. Space-efficient fair packet sampling algorithm[J]. Journal of Software, 2010, 10: 2642-2655.)

[5] 王洪波,程时端,林宇. 高速网络超连接主机检测中的流抽样算法研究[J]. 电子学报,2008(4):810-818. (WANG H B, CHENG S D, LIN Y. On flow sampling for identifying super-connection hosts in high speed networks [J]. Acta Electronica Sinica, 2008(4): 810-818.)

[6] 孙昱,夏靖波,赵小欢,等. 基于 LEAST 和 CBF 两级结构的大流检测算法[J]. 华中科技大学学报:自然科学版,2014,42(4):40-44. (SUN Y, XIA J B, ZHAO X H, et al. LEAST and CBF two-level architecture based algorithm for identifying and measuring large flows[J]. Journal of Huazhong University of Science and Technology: Natural Science Edition, 2014, 42(4): 40-44.)

[7] 胡广昌. 基于 Bloom Filters 流抽样算法的研究[D]. 曲阜:曲阜师范大学,2010. (HU G C. The flow sample algorithm research based on Bloom Filters[D]. Qufu: Qufu Normal University, 2010.)

[8] HUBER J. Design of an OC-192 flow monitoring chip[M]. San Diego: University of California, San Diego Class Project, 2001.

[9] VOELKER G M, SAVAGE S. Cooperative association for Internet data analysis[EB/OL]. [2014-06-23]. http://www.caida.org/.

[10] 张震,汪斌强,张风雨,等. 基于 LRU-BF 策略的网络流量测量算法[J]. 通信学报,2013,34(1):111-120. (ZHANG Z, WANG B Q, ZHANG F Y, et al. Traffic measurement algorithm based on least recent used and Bloom filter[J]. Journal on Communications, 2013, 34(1): 111-120.)