# 基于掩码匹配的报文双抽样方法

夏靖波[1]， 孙 昱[1]， 申 健[1]， 王少龙[1]， 王 芳[2]
(1.空军工程大学信息与导航学院,陕西西安,710077;2.空军大连通信士官学校，辽宁大连,116000)

**摘要** 基于掩码匹配的报文抽样算法是一种实用性较强的分布式流量抽样算法,但是该算法在测量报文到达时间间隔的分布这一重要网络流量特征时性能较差。首先根据误差理论分析了产生这一问题的原因,为了降低测量的系统误差,在原算法中引入了双抽样的改进方案。考虑到改进后的算法会给测量系统带来额外的负担,提出了增加了抽样掩码位数的解决办法,并且论证了其可行性。最后基于实际的网络流量数据进行了实验验证,结果表明:改进后的算法测得的报文到达时间间隔的分布符合真实的分布情况,并且对其它网络性能指标的测量精度影响较小。

**关键词** 流量测量;掩码匹配;报文到达时间间隔;双抽样;测量精度
**DOI** 10.3969/j.issn.1009-3516.2013.04.013
**中图分类号** TP393　　**文献标志码** A　　**文章编号** 1009-3516(2013)04-0052-05

## A Packet Double Sampling Method Based on Mask Matching

XIA Jing-bo[1], SUN Yu[1], SHEN Jian[1], WANG Shao-long[1], WANG Fang[2]

(1. Information and Navigation College, Air Force Engineering University, Xi′an 710077, China;
2. Dalian Air Force Communications NCO Academy, Dalian 116000, China)

**Abstract**: The packet sampling algorithm based on mask matching is a practical distributed traffic sampling algorithm. But the algorithm is ineffective in measuring an important network traffic characteristic, which is the distribution of packet arrival time interval. First of all, the reason leading to the problem is analyzed according to the error theory. Then, an improved program of double sampling is introduced in the initial algorithm in order to reduce the system error of measurement. As the improved algorithm will bring extra burden to the measurement system, a solution which is to increase the sampling mask bits is put forward and its feasibility is demonstrated. Finally, the improved algorithm is tested with the actual network traffic data. The experiment results show that the measurement of the distribution of packet arrival time interval is in line with the real situation. And it has little effect on the measurement accuracy of other network performances.

**Key words**: traffic measurement; mask matching; packet arrival time interval; double sampling; measurement accuracy

网络流量测量和分析是研究网络行为学的基础,通过测量和分析,可以掌握网络行为的基本特

**收稿日期**:2013-01-26
**基金项目**:陕西省自然科学基金资助项目(2012JZ8005)
**基金项目**:夏靖波(1963—),男,河北秦皇岛人,教授,博士生导师,主要从事通信网络管理与评估研究.
E-mail:jbxiad@sina.com

征,构造出反映网络行为的数学模型,为网络的有效管理、合理利用提供有力的理论支持和科学依据。由于高速网络技术的发展,要捕获流经链路的所有数据分组相当地困难,并且需要巨大的开销,所以,报文抽样技术成为了目前在高速链路上进行流量测量的主要解决方案[1]。

传统的报文抽样方法包括系统抽样,随机抽样和分层抽样,其中的泊松随机抽样[2]是 RFC2330 文档中推荐使用的抽样方式。这几种传统的抽样方法都简单易于实现,而且对各个主要的网络性能指标的测量效果比较好。为了能更精确地测量被关注的网络性能指标,自适应抽样[3-6]逐渐发展了起来。该类抽样方法利用网络流量的相关性动态预测流量状态,并通过实时调整抽样策略或参数更好地捕捉流量特征,从而对所关注的网络性能指标能达到更 高的测量精度。但是这些抽样方法均不满足抽样报文的一致性,即若某个报文被网络中的一个测量节点抽中时,并不能保证其它的测量节点也会抽中该报文。这样,对于一些需要各个测量节点相互协作才能完成的测量任务,例如报文的传输延迟,报文的传输路径等,这些抽样方法都无能为力。

基于掩码匹配的报文抽样算法[7-8]利用事先选定的掩码与报文中不随传输发生变化的字段进行模式匹配,当匹配结果一致时,该报文被抽样,否则该报文不被抽样。如果网络中所有的测量节点均使用相同的抽样掩码,那么当某个报文被一个测量节点抽中时,它也会被其它节点抽中,否则所有节点都不会抽中它,因而能较好地满足抽样报文的一致性。但是,该算法对报文到达时间间隔的分布这一重要的网络流量特征的测量效果并不令人满意,因此,本文将对其进行改进,在不影响该算法对其它网络性能指标的测量精度的前提下,提高它对报文到达时间间隔的分布的估计精度,从而增强该算法的测量性能,使之能更准确地反映出网络的整体运行状态。

# 1　算法分析

根据掩码匹配抽样[8]的原理,这类算法获得的样本的随机性好坏在很大程度上依赖于报文中用于模式匹配的目标字段的随机性好坏。文献[8]的研究表明,在 IPv4 网络中,报文 IP 头部里面的 16 位标识字段随机性最佳,所以该字段常被用作掩码匹配的目标字段。这样得到的样本虽然对网络流量负载、吞吐量等网络性能指标的估计精度较高,但是对报文到达时间间隔的分布进行估计时测量误差却比较大,原因如下所述。

要估计报文到达时间间隔的分布律,首先需要得到报文到达时间间隔的样本。但是该抽样算法获得的报文样本是由若干个 IP 报文组成,并没有报文到达时间间隔的直接测量量,所以若需要报文到达时间间隔只能采取间接计算的办法。如果报文样本中相邻两个报文到达的时间间隔为 $t$,抽样间隔为 N 个报文,那么可以得到一个报文到达时间间隔的估计值 $t/\mathrm{N}$。当报文样本的容量为 $n+1$ 时,利用其中每对相邻的报文都可以计算得到一个报文到达时间间隔,这些报文到达时间间隔组成的样本的容量为 $n$。使用它对报文到达时间间隔的分布律进行估计时,若其中有 $m$ 个样本点落在选定的时间区间内,那么报文到达时间间隔在该区间出现的概率为 $p=m/n$。由于所使用的样本值不是直接测量量,而是间接计算量,因此在计算分布概率 $p$ 时,受误差传递效应的影响,偏差往往很大。

计算结果的误差可分为系统误差和随机误差两类,系统误差由报文到达时间间隔样本本身是估计值引起,随机误差由抽样报文的随机性引起。假设系统误差的极限误差是 $e$,随机误差的极限误差是 $\delta$,那么按照极限误差的合成公式[9],估计概率 $p$ 的极限误差为:

$$\Delta=\pm s\sqrt{\left(a\frac{e}{t}\right)^2+\left(a\frac{\delta}{t}\right)^2} \tag{1}$$

式中:$a$ 为误差传递系数;$t$ 为置信系数;$s$ 为总误差的置信系数。因此若要提高报文到达时间间隔的分布的测量精度,根据上式必须降低系统误差与随机误差,即:①报文到达时间间隔的样本应使用准确值而非估计量;②报文到达时间间隔的样本应随机性良好。

# 2　算法改进

## 2.1　算法流程

报文到达时间间隔的准确值可以通过抽样 2 个连续的报文获得,所以,当掩码匹配一致成功抽中一个报文时,若其后续的那个报文也能被抽中,那么,通过这 2 个报文就可以获得一个报文到达时间间隔的直接测量量。

因为掩码匹配抽样是使用 IP 报文中随机性较好的标识字段作为匹配的目标字段,所以这些匹配成功的报文组成的样本具有较好的随机性。而通过连续 2 个报文获得的每一个报文到达时间间隔的测量量都与该样本中相应的一个报文有关联,因此这些报文到达时间间隔的测量量组成的样本也将具有较好的随机性。当用该样本来估计报文到达时间间

隔的分布律时,准确性会得到较大的提高。

按上述思想对原算法[8]进行改进,改进后的算法流程见图 1。

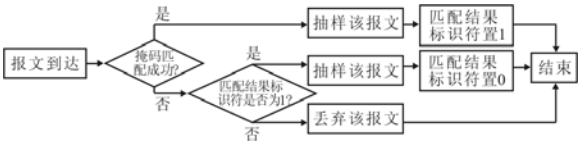


图 1 基本的算法流程

Fig. 1 The basic algorithm process

改进算法通过设置一个匹配结果标识符,保证当一个报文由于掩码匹配成功被抽中时,它后续的这个报文也能被抽中,这样将能得到一个准确而且随机性较好的报文到达时间间隔的样本。

### 2.2 掩码长度的选择

假设 IP 报文中用作掩码匹配的目标字段完全随机,那么当原算法使用 $n$ 位掩码进行匹配抽样时,抽样率为 $1/2^n$,将其获得的样本称为固有样本。如果改进算法使用同样的 $n$ 位掩码进行匹配抽样,那么它所获得的样本可以分为两部分。一部分是由于掩码匹配成功抽中的,即和原算法一样的固有样本;另一部分是虽未匹配成功,但是为了得到报文到达时间间隔的准确值也被抽中的,这部分样本称为附加样本。由于附加样本的存在,同样是使用 $n$ 位掩码,改进算法的抽样率将大于原算法的抽样率。如果原算法使用的掩码长度是根据链路带宽,测量节点的处理能力等因素设置的,那么当改进算法使用相同长度的掩码时,由于其抽样率更高,需要处理的报文数更多,将有可能发生测量节点处理速度跟不上报文到达速度的情况,造成抽中报文的丢失,给各个测量指标的估计带来不利的影响。因此,为了避免这一情况的发生,当原算法采用 $n$ 位掩码进行抽样测量时,改进算法将采用 $n+1$ 位掩码进行抽样测量以降低其抽样率。

下面利用实际的网络流量数据来验证这一点,这些数据为 MAWI 工作组[10]在互联网骨干链路上测得,每组数据有超过 $10^6$ 个报文。分别使用原算法和改进算法进行抽样,计算实际抽样率见图 2。

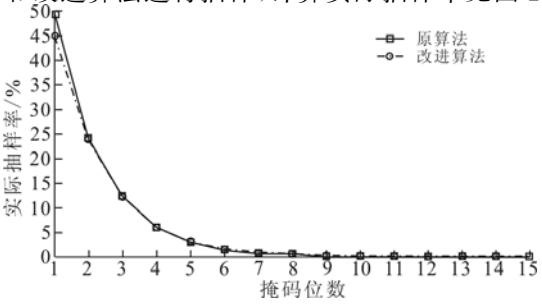


图 2 实际抽样率比较

Fig. 2 The comparison of actual sampling rate

当原算法采用 $n$ 位掩码抽样时,改进算法采用 $n+1$ 位掩码抽样,所以改进算法得到的固有样本容量为原算法得到的固有样本容量的一半。当抽样掩码长度较长时,由于抽样率较低,固有样本中的报文平均抽样间隔较长,因此当固有样本每增加一个报文时,改进算法为了得到相应报文达到时间间隔的准确值,附加样本也将增加一个报文,此时附加样本容量几乎等于固有样本容量,这样,改进算法采用 $n+1$ 位掩码抽样得到的样本总数(固有样本与附加样本之和)与原算法采用 $n$ 位掩码抽样得到的样本总数几乎相同,二者的实际抽样率几乎一样。而当掩码长度较短时,固有样本中的报文平均抽样间隔较短,很有可能当一个报文匹配抽中时,下一个报文也正好匹配抽中,这样前一个报文对应的报文到达时间间隔的准确值通过固有样本就能得出,不必在附加样本中多增加一个报文,此时,附加样本容量将小于固有样本容量,所以改进算法实际抽样率会略小于原算法。

由于改进算法的实际抽样率不高于原算法,故改进算法具有可行性。

### 2.3 目标字段的选择

根据掩码匹配抽样的原理,固有样本随机性的好坏主要取决于报文中用于匹配的目标字段随机性的好坏,而报文到达时间间隔样本的随机性好坏又与固有样本随机性的好坏有直接的关系。因此,若能提高目标字段的随机性,最终在估计报文到达时间间隔的分布时,其测量精度也能获得提高。

为了衡量目标字段的随机性好坏,首先定义信息熵的概念。

定义:记一个 $m$ 位的二进制序列 $a_1 a_2 \cdots a_m$ 为 $s$,$s$ 共有 $n=2^m$ 种取值可能,若每种取值的概率分别为 $p_1, p_2, \cdots, p_n$,则 $s$ 的熵为 $H(s)=-\sum_{i=1}^{n} p_i \log_2 p_i$。

目标字段的熵越大,则说明该字段越随机。

由于报文 IP 头部中的 16 位标识字段被证明具有良好的随机性[8],所以基于掩码匹配的抽样算法通常将该字段用作匹配的目标字段。笔者分别统计了 10 组流量数据,每组流量数据有 $10^6$ 个数据包,发现报文 IP 头部中的标识字段在与 32 位的目的 IP 字段的后 16 位作异或运算后,所得结果的熵更高,随机性更好,将二者异或运算的结果称为新标识字段,统计结果见图 3。

无论标识字段还是新标识字段,它们都是 16 位的二进制串,故其熵的最大值[11]为 16。从图 3 中可以看出,标识字段的熵已经很高,证明该字段确实具备良好的随机性,但是异或得到的新标识字段的熵

比它更高,随机性更强。因此,改进算法在进行掩码匹配时,先将从到达的报文的 IP 头部中提取出标识字段和目的 IP 字段的后 16 位,然后将二者进行异或运算,最后使用掩码对异或的结果进行匹配,如果一致则抽样。

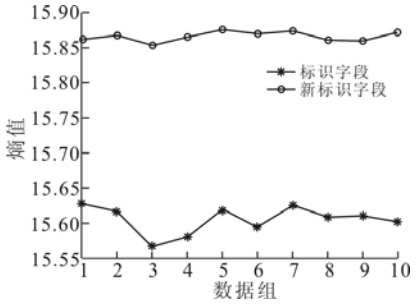


图 3　熵值比较

Fig. 3　The comparison of entropy

## 3　实验验证

本文实验所用数据同样来自 MAWI 工作组在互联网骨干链路上全流量采集获得,共 8 组,每组流量数据持续的时间为 100 s。

### 3.1　报文到达时间间隔的分布

由于所用流量数据中报文到达时间间隔多在 0～500 us 之间,将其分为 50 个区间,每个区间 10 us,500 us 以上的到达时间间隔单独作为一个区间。如果总体中报文到达时间间隔落在这 51 个区间的概率分别为 $p_i(1\leqslant i\leqslant 51)$,样本中到达时间间隔落在这 51 个区间的概率分别为 $q_i(1\leqslant i\leqslant 51)$,样本容量为 $n$,那么可以计算卡方检验量[11] $\chi^2=\sum_{i=1}^{51}\frac{n}{p_i}(q_i-p_i)^2$ 来观察样本分布是否符合总体分布。

分别使用原算法和改进算法对这 8 组流量数据中报文到达时间间隔的分布进行估计。原算法最后计算得到的卡方值的数量级均在 $10^3$ 以上,无法通过卡方分布检验,而改进算法所得结果见图 4。

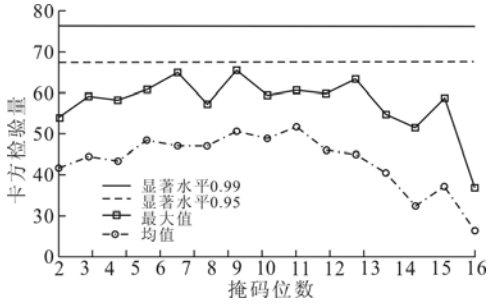


图 4　卡方检验值

Fig. 4　The chi-square value

从图 4 中可以看出,即使是 8 组流量数据中卡方检验量 $\chi^2$ 的最大值也能通过显著性水平为 0.05 和 0.01 的检验,这说明了改进算法对报文到达时间间隔的分布的估计符合真实情况,证明了该改进方案的有效性。

### 3.2　网络流量负载的测量精度

下面观察改进算法对其它网络性能指标的测量精度是否受到影响,以网络流量负载的测量为例。改进算法得到的报文样本分为固有样本和附加样本 2 种。在对流量负载进行估计时,由于不能保证固有样本和附加样本二者构成的总体依然保持较好的随机性,因此与原算法一样,仅使用固有样本进行估计。但是由于改进算法采用的掩码长度比原算法更长,得到的固有样本容量更低,这很可能导致对流量负载的估计精度下降。但是,如果流量负载的估计精度下降的幅度可以接受,那么改进算法仍然是可行的。

当抽样算法采用的掩码长度为 $n$ 时,若获得的固有样本的总字节数为 $k$,那么,对流量负载真实值 $K$ 的估计值为 $K'=k/(1/2^n)=k2^n$,相对误差 $e=|K-K'|/K$。分别使用原算法和改进算法对实际流量数据进行抽样,计算流量负载估计的相对误差,结果见图 5。

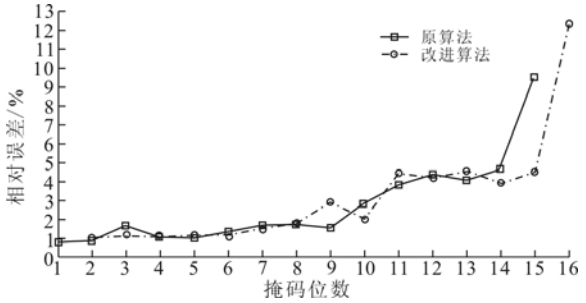


图 5　流量负载相对误差比较

Fig. 5　The comparison of traffic load relative error

图 5 中所得相对误差为 8 组数据的均值,从图中可以看出,虽然改进算法使用的掩码位数更多,获得的固有样本更少,但是其测量精度与原算法相比,下降的并不多。事实上,当掩码位数一定时,如果报文总体中的报文数量提高(例如将原算法与改进算法应用于更高速的网络中),那么二者的差距将更小。因此,改进后的算法几乎不会影响到对其它网络性能指标的测量。

## 4　结语

作为一种分布式的报文抽样算法,掩码匹配抽样具有比较全面的测量能力。本文通过分析其在测量报文到达时间间隔的分布上的不足,引入了报文双抽样的解决方案,从而较好地解决了这一问题,进一步增强了该算法的测量性能。改进后的算法不仅

简单易于实现,而且能够更加准确地反映出网络的整体运行状况,具有良好的实用性。

**参考文献(References):**


[1] 程光,龚俭.大规模高速网络流量测量研究[J]. 计算机工程与应用,2002,39(5):17-19.
CHENG Guang, GONG Jian. A research on traffic measurement in a large-scale high-speed network[J]. Computer engineering and applications, 2002, 39(5): 17-19. (in Chinese)

[2] 张峰,雷振明. 基于泊松分布的报文抽样性能衡量[J]. 北京邮电大学学报,2005,28(2):34-38.
ZHANG Feng, LEI Zhenming. The evaluation of poisson-based packet sampling techniques[J]. Journal of Beijing university of posts and telecommunications, 2005, 28(2): 34-38. (in Chinese)

[3] 陈松,王珊,周明天. 基于实时分析的网络测量抽样统计模型[J]. 电子学报,2010,38(5):1177-1180.
CHEN Song, WANG Shan, ZHOU Mingtian. Network data measurement and statistics model based on real-time analysis[J]. Acta electronica & sinica, 2010, 38(5): 1177-1180. (in Chinese)

[4] 潘乔,罗辛,王高丽,等. 基于 FARIMA 模型的流量抽样测量方法[J]. 计算机工程,2010,36(15):7-11.
PAN Qiao, LUO Xin, WANG Gaoli, et al. Traffic sampling measurement method based on FARIMA model[J]. Computer engineering, 2010, 36(15): 7-11. (in Chinese)

[5] 陈庶樵,张果,朱柯. 一种基于包速率自适应的报文抽样算法[J]. 计算机应用研究,2010,27(7):2727-2729.
CHEN Shuqiao, ZHANG Guo, ZHU Ke. Algorithm based on packet rate adaptive for packet sampling[J]. Application research of computers, 2010, 27(7): 2727-2729. (in Chinese)

[6] 刘元珍,刘渊,李小航. 自相似网络的自适应系统双抽样方法研究[J]. 计算机工程与设计,2007,28(22):5409-5410.
LIU Yuanzhen, LIU Yuan, LI Xiaohang. Study on self-adaptive systematic double sampling method for self-similar network traffic[J]. Computer engineering and design, 2007, 28(22): 5409-5410. (in Chinese)

[7] 潘乔,裴昌幸. 基于信息熵理论的高速 IPv6 网络流量抽样测量方法[J]. 吉林大学学报:工学版,2009,39(5):1338-1341.
PAN Qiao, PEI Changxing. Information entropy theoretic approach to traffic sampling measurement in high-speed IPv6 networks[J]. Journal of Jilin university: engineering and technology edition, 2009, 39(5): 1338-1341. (in Chinese)

[8] 程光,龚俭,丁伟. 基于统计分析的高速网络分布式抽样测量模型[J]. 计算机学报,2003,26(10):1266-1273.
CHENG Guang, GONG Jian, DING Wei. Distributed sampling measurement model in a high speed network based on statistical analysis[J]. Chinese journal of computers, 2003, 26(10): 1266-1273. (in Chinese)

[9] 沙定国. 误差理论与测量不确定度评定[M]. 北京:中国计量出版社,2003.
SHA Dingguo. The error theory and measurement uncertainty[M]. Beijing: China metrology press, 2003. (in Chinese)

[10] MAWI working group traffic archive. Traffic trace info [EB/OL]. (2013-01-26). http://mawi.wide.ad.jp/mawi.

[11] 程光,龚俭. 互联网流测量[M]. 南京:东南大学出版社,2008.
CHENG Guang, GONG Jian. Internet flow measurement[M]. Nanjing: Southeast university press, 2008. (in Chinese)


(编辑:徐楠楠)