基于统计分析的高速网络分布式抽样测量模型✍

程光，龚俭，丁伟
（东南大学计算机科学与工程系　南京　210096）
(江苏省计算机网络技术重点实验室　南京 210096)

摘要：分布式被动测量是研究网络行为的一个重要手段，其面临的主要问题是难以实现高速网络流量测量，因此需要使用抽样技术。分布式抽样测量技术需要解决两个关键问题：分布式测量点测量报文的一致性和抽样样本的统计随机性。为此，抽样测量的核心是选择合适的抽样掩码匹配位串，以保证抽样样本的随机性，且实现分布式测量点的信息一致性。文章对 CERNET 主干网络流量 IP 报头各字段的随机性进行分析，结果表明标识字段 16 比特满足抽样掩码匹配位串要求。并对抽样样本的随机性和统计属性进行分析，实验验证抽样样本既能用于网络行为研究也能用于流量行为研究。

关键词：抽样测量，抽样掩码，位熵，标识字段
中图法分类号： TP393　　**文献标识码：**A

1、 引言

网络类似于人类社会，虽然是由人所创造，但具有不以人的意识为转移的客观规律。网络行为学就是研究网络客观规律的科学，使人类能更充分了解、应用发展网络。近十年来，由于网络的飞速发展，网络行为变得越来越复杂，面临的问题越来越多，因此网络行为规律成为网络研究的重点[1]。研究网络规律首先要了解网络行为，网络测量是基础。网络流量测量主要有两种方法：主动测量和被动测量。主动测量[2]在测量过程中向网络注入用于测量网络特性的流量，是一种干扰性测量方法，测试流量产生的附加荷载可能会影响网络链路、路由器的性能状况，最终可能影响测量结果。被动测量[3]直接利用网络中已有的流量，是一种非干扰性测量方法，但被动测量面临高速流量荷载问题，难以实现流量实时测量和处理。目前的被动测量研究基本是属于单点测量，主要用于计费、统计分析及入侵检测等应用。但有的网络规律研究（如：网络路由行为、网络端至端性能行为）需要多点协同测量数据，因此近几年国外出现一些分布式被动测量体系结构[4-6]。

为了解决高速网络被动测量问题，早在 1993 年，Claffy[7]测量 NSFNET 主干流量时，使用基于事件和时间驱动的静态抽样方法。RFC2330[8]分析抽样测量的随机性，推荐使用泊松抽样方法实现网络流量抽样测量。这些的抽样模型只适用于单点被动测量，为了能在分布式体系结构中使用抽样技术，Cozzani[6]测量 ATM 位元时使用校验和字段模式匹配实现抽样，但从其文章研究来看，校验和的随机性并不理想，且 IP 分组的校验和字段在传输过程中发生变化，无法实现分布式测量点抽样同样 IP 报文。Duffield[5] 提出对 IP 分组传输中不变的字段使用哈希函数实现抽样，哈希函数不能保证样本的随机性，模数难以确定，且抽样算法运算较为复杂、时间复杂度大，难以实现高速网络环境中实时抽样测量。

文章研究在分布式被动测量环境中的抽样测量模型，保证分布式测量体系结构协同不同测量点的一致性报文信息来实现性能分析，即对于任意一个通过测量域的报文，该报文要么被其通过的所有测量点所俘获，要么没有一个测量点俘获该报文。将抽样技术用于高速网络测量，可以在满足问题统计精度的条件下，减少用于测量、存储和处理的数据量。抽样技术体现随机性，但为了协同分布式测量点数据，抽样模型又要具有确定性。为此，文章对通过

✍基金项目：本文受国家自然科学基金重点课题“90104031”和国家 863 课题“2001AA112060”资助

CERNET 主干数亿个 IP 报文统计分析，提出一种抽样掩码匹配测量模型，其核心是寻找抽样掩码匹配位串，通过统计分析，发现 IP 报文标识字段是掩码匹配理想位串。这个模型能保证抽样样本统计上的随机性，又能实现分布式测量点之间的一致性。

文章首先定义评价报文字段随机性的测度，并提出抽样掩码测量模型；接着基于统计随机性测度，寻找抽样掩码匹配的理想位串——标识字段；然后基于模型的抽样样本进行统计估计分析，以证明抽样样本能估计流量总体特性；最后总结研究内容。

2、 分布式抽样测量模型

2.1 概念定义

在分析抽样测量模型之前，需要引入评价随机性的测度标准，熵[9]是信息论中的基本概念，可用于评价各种随机试验不确定程度，因此可用于度量 IP 分组各比特的随机性。文章将熵的概念推广应用研究比特随机性，下面定义和抽样测量模型有关的一些重要概念。

定义 1，位熵，一个比特所表示的信息量，比特 b 具有 0、1 两种可能性，设其概率分别为 p_0、p_1，则位熵 H（b）定义为：$H(b) = -(p_0 \log_2 p_0 + p_1 \log_2 p_1)$。 （1）

定理 1，最大位熵定理。由最大熵定理[12]可知，如果比特 b 中 0、1 事件以等概率出现，即当 $p_0 = p_1 = 1/2$，其熵最大，故最大位熵 $H_{\max}(b) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1$，也就是位熵最大值为 1。

定义 2，比特随机测度 E。定义实际位熵 H（b）和最大位熵 H_{max}（b）的比值，即 $E = H(b)/H_{\max}(b) = H(b)$。由于最大位熵为 1，所以比特随机测度值就等于位熵的值。由定义可知，$0 \le E \le 1$，E 表示随机程度，E 越接近 1 表示信息越随机，位熵越大，E 接近 0，表示确定性信息越大，位熵越小。

定义 3，比特确定测度 R。定义为（1-E），表示比特信息确定性的程度。因为确定性是不含有信息量，所以比特确定测度值 $R=1-E=1-H(b)/H_{max}(b)=1-H(b)$。

2.2 抽样测量模型

高速 IP 流量抽样测量的目的是抽取流量子集来实现对总体流量信息的估计，抽样理论建立在抽样样本随机性基础上，样本的随机程度越大，对总体信息估计就越精确。抽样理论要求抽样样本需要具有随机性的特征，因此，针对大规模高速 IP 网络流量抽样测量，我们认为可以有二种抽样方法：一种是目前被动抽样测量中主要采用的技术，如 RFC2330 定义的泊松抽样模型。抽样测量算法随机生成一个抽样事件，如以确定的计时器或计数器溢出作为激发抽样的事件，抽样算法在报文到达之前就已经决定其是否被抽样，这种抽样方法不能实现分布式协同，只适用于单点测量体系结构。第二种是抽样事件事先确定，在报文到达之前是不能确定其是否被抽样，只有当报文到达以后根据报文内容才能决定抽样与否。确定的抽样事件能保证分布式测量点之间的协同，但难以保证抽样样本之间的统计随机性，因此该方法的核心是抽样事件的生成算法，其中随机性和效率是生成算法性能的两个关键指标。

分布式测量体系结构中，抽样是从通过网络的报文中随机选择部分报文，第一种抽样方法不能保证分布式测量点从同样的流量中抽取相同的样本，不同的抽样样本无法实现网络行为分析。因此，保证分布式测量点能获得一致性报文信息，只能使用第二种抽样测量方法，使用确定的抽样模型，由指定的报文具体内容激发报文抽样。同第一种方法相比，第二种抽样方法样本的随机性无法用数学理论证明，只能通过对实测报文统计分析来确定。

文章所研究的是内容激发的抽样测量模型，根据报文的某些位具有随机性，使用指定的掩码和指定的比特串相匹配以实现抽样，抽样方法的核心是选择合适的报文匹配比特串，这些比特必须在统计上具有随机性，同时又和流量统计特性无关。这样既能保证分布式测量点抽样到同样的报文，又能实现抽样报文样本统计的随机性。

如果一个抽样掩码和指定的报文比特串发生匹配，那么测量器将抽样该报文。如果在测量体系结构中所有测量器的匹配函数使用相同的抽样掩码，指定相同的匹配比特串，就能实现分布式测量体系结构中抽样测量一致性报文流量。这种匹配机制以比特为基础，使用一个内容随机的比特掩码比较每个报文中的指定比特的内容，比特掩码的偏移和长度决定测量体系结构的精度和可靠性，图 1 显示一个抽样掩码来实现掩码匹配的抽样测量。假设被匹配的每个比特出现 0 和 1 的概率类似于掷硬币，等概率随机分布，即 0 和 1 出现的概率均为 1/2，同时假设不同比特间服从独立同分布，则理论上抽样比率是由抽样掩码比特长度决定的，理论抽样比率 ratio=$1/2^n$。但报文中匹配比特串的每一比特很难保证等概率随机分布且独立同分布，实际抽样比率同被选取的匹配比特串是有直接关系，被匹配位串的比特随机测度值越接近 1，则实际抽样比率越接近理论抽样比率。因此模型的核心是寻找合适的被匹配比特，选择的比特必须满足以下几方面因素：1、被匹配的比特在传输过程中不能发生变化，这是实现分布式协同抽样测量的首要条件；2、被匹配的比特需要具有高随机性，使得实际抽样比率在概率范围内等于理论抽样比率；3、被匹配的比特尽可能与报文统计属性无关。下面定义 3 个函数理论描述满足上述 3 个条件的抽样模型。假设报文内容表示为 X 比特串。

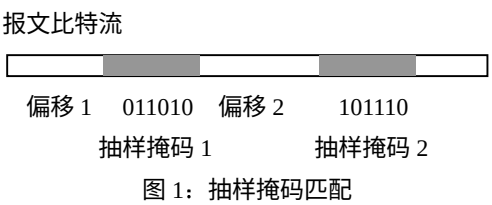

图 1：抽样掩码匹配

定义 4，恒定函数 S，函数 S 输出的结果是在传输过程报文中不变的部分，即分组在传输过程中，不被修改的位串。如果没有丢失产生，假设函数 S 能提取分组中所有不变的位串 X_C，$S:\{0,1\}^X \rightarrow \{0,1\}^{X_C}$。满足条件 1。

定义 5： 确定函数 H，分布式抽样测量的基本思想是使用一个确定的抽样函数 H，从报文不变字段 X_C 中提取高位流熵 X_l 位串，$H:\{0,1\}^{X_C} \rightarrow \{0,1\}^{X_l}$。满足条件 2、3。

定义 6：抽样函数 H_D，$H_D(S(X))=\begin{cases}1, & H(S(X))=D\\ 0, & H(S(X))\neq D\end{cases}$，如果抽样函数 H_D（ ）=1，那么将抽样该报文，否则将抛弃。实现抽样。

采用抽样掩码匹配测量模型，容易保证分布式测量点之间抽样的一致性，但难以保证样本随机性，X_l 位串的随机性无法通过数学理论证明，只能通过流量统计分析来证明。下面将对通过 CERNET 国家主干报文比特的位熵进行分析，选取比特随机测度值大的比特作为 X_l 位串，并根据抽样精度要求选择 D 的取值范围。

3、流量比特统计分析

3.1 IP 报头位熵分析

恒定函数 S 将报文 X 位流映射为不变位串 X_C，确定函数 H 将不变位串 X_C 映射为熵值最大的位串 X_l，这些映射函数不能

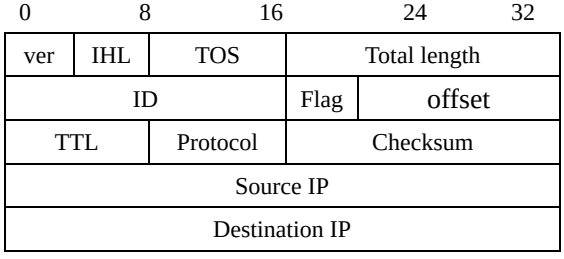

图 2 IP 报头组成

只通过数学公式推导出来，需要通过大量报文统计分析才能得到。文章使用千兆光纤网卡、PIII 1G CPU、Red Hat6.2 操作系统，开发可以直接测量 CERNET 主干链路流量的测量器，并对 100,000,000 个 IP 报文头前 20 个字节、160 比特的位流进行统计分析。图 2 是 IP 报头的组成。

版本号字段(version)记录报文的版本协议，占有 4 个比特，但测量的所有报文均是 IPv4。因此，其各比特随机测度值 E＝0，比特确定测度值 R＝1，也就是 4 个比特表示的是确定值，不包含任何信息。测量的所有报文中 IHL 字段长度均为 5，也就是说目前几乎没有 IP 报文使用选项字段，所以 IHL 字段表示的也是确定值。

服务类型字段 8 位中 1～3 位表示优先顺序字段，目前仅有 0.021％的报文标志了优先级信息。4～6 位表示标志位，通过测量分析可知 2.55%的报文标志延迟，2.98％的报文标志吞吐量，0.03％的报文标志可靠性，它们对应的比特随机测度值分别为 0.171、0.193、0.004。最后 2 位目前没有定义，在 100,000,000 个报文中，仅有 40 个报文使用了这两位。该字段 E 值很低，同时还可能会被通过的某些路由器所改变。

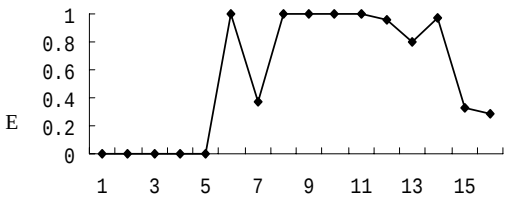

图 3 报文长度字段比特随机测度

总长字段 16 位，目前 IP 网络中的报文长度集中在 40、552、576 和 1500 字节[1]，其比特随机测度 E 见图 3。由于最大长度字段受网络限制，因此，长度字段的前 5 个比特随机测度值为 0，第一个字节的位熵变化较大，且信息效率较低，不适合作为抽样匹配位串，第二个字节位熵信息效率基本接近 1，可以考虑作为抽样匹配位串。但如果报文通过测量域中出现分段，那么长度字段将发生变化。

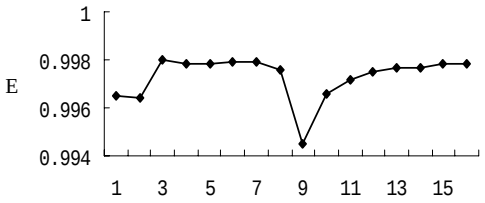

图 4 标识字段比特随机测度值

标识字段用来让目的主机判断新来的分段属于哪个分组，所有属于同一分组的分段包含同样的标识值，因此，标识字段在传输过程中不管是否出现分段均不会发生变化，图 4 是标识字段的比特随机测度图。标识字段中的 16 位比特测度值均在大于 99％，同时标识字段在传输过程中不发生变化，因此使用标识字段作为抽样匹配位串相当适合。

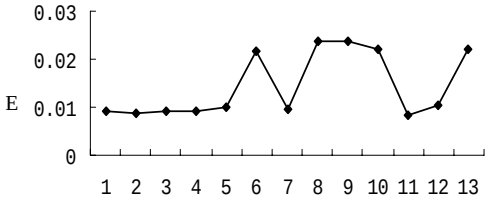

图 5 分段偏移字段比特随机测度

Flag 字段中，88.7％的报文标识 DF 位。0.31％的报文标志 MF 位。图 5 表示 offset 字段的比特随机测度值，各比特随机性较低，且传输过程中可能发生变化,不适合作抽样匹配位串。

生存期（TTL）字段是用来限制分组生命周期的计数器，它每经过一个路由器都会递减，因此，不适合考虑作为抽样掩码匹配位串。协议字段说明报文将送给那个传输进程，对网络流量统计分析表明：TCP（6）[10]占 93.04％的报文，UDP（17）占 6.37％，其它所有协议总共占 0.59％，因此，协议字段的随机性较小，

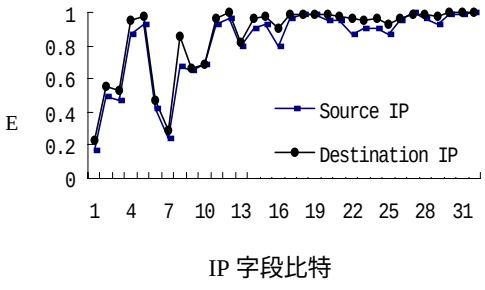

图 6 IP 字段比特随机测度

比特确定测度值较大。头校验和字段仅用于校验头部，因为每通过一个路由器，至少有一个字段（生存期）发生变化，所以校验和字段每通过一个路由器都在发生变化，不适合作为抽样掩码匹配位串。

源 IP 和宿 IP 在传输过程中不发生变化，图 6 是 IP 字段比特随机测度图。由于 CERNET 网络中的流量主要集中在少数一些网络号中，因此，32 位的 IP 地址中前 16 比特随机测度值较低，比特确定测度值较大，而后 16 位主要是主机号，变化较为随机，其比特随机测度值较大。由于后 16 个字节中全 0 和全 1 有特殊用途，故在网络流量中存在这两种情况的冗余。从图 6 可以看出，IP 字段前 16 比特随机测度值较小，变化幅度较大，而后 16 位字节变化幅度不大，每位比特随机测度值在 90%。源/宿 IP 字段后 16 位在传输过程中不发生变化，且比特随机测度值较大，故源 IP 和宿 IP 的后 2 个字节中的 16 比特可以考虑作为抽样掩码匹配位串。

3.2 比特流随机测度分析

根据以上对 IP 报头各字段的比特随机测度统计分析，标识字段 16 比特、源 IP 后 16 比特和宿 IP 后 16 比特具有在传输过程不发生变化且比特随机高的特点，初步选定这 3 个位串可以作为抽样掩码匹配位串，但上文只是单独考虑比特随机测度值的大小，没有考虑不同比特是否存在相关关系，因此需要分析这 3 段 16 比特串中各比特之间的相关关系。下面先给出位流熵定义、最大位流熵定理以及比特流随机测度。

定义 7 位流熵是比特流所表示的信息量，比特流 s 具有 $n+1=2^s$ 种可能性，设其概率分别为 p_0、p_1、…、p_n，则位熵 H（s）定义为：

$$H(s) = -\sum_{i=0}^{2^s-1} p_i \log_2 p_i \qquad (2)$$

定理 2：最大位流熵定理：由最大熵定理[12]可知，如果比特流 s 中 2^s 种事件以等概率出现，即当 $p_0=p_1=\cdots=p_n=1/2^s$ 时，其熵最大，故 $H_{\max}(s) = -\sum_{i=0}^{2^s-1} \frac{1}{2^s} \log_2 \frac{1}{2^s} = s$。

定义 8：比特流随机测度 E：实际位流熵 H（s）和最大位流熵 H_{max}（s）的比值，表示比特流随机程度，$E = H(s)/H_{\max}(s) = H(s)/s$。

从 CERNET 主干网络某处，在不同的时间分 10 次测量 IP 流量，每次测量 10,000,000 个报文，分析每组 IP 报文的标识字段 16 比特、源 IP 后 16 比特和宿 IP 后 16 比特的比特流随机测度值，三组测度值比较见图 7。标识字段 16 比特的最小比特流随机测度值 E=0.901，最大 E=0.915，变化幅度为 0.014；宿 IP 后 16 比特的最小 E=0.648，最大 E=0.668，变化幅度为 0.020；源 IP 后 16 比特的最小 E=0.544，最大 E=0.556，表明大规模网络流量位流熵统计上的稳定性，根据平稳特性，可以选用部分比特作为抽样掩码匹配位串以实现统计上的随机特性。对 3 种比特流的 E 值分析表明，标识字段 16 比特位流熵值最大，因此选用标识字段 16 比特中的部分比特作为抽样掩码匹配比特串能很好的实现抽样样本的统计随机特性。

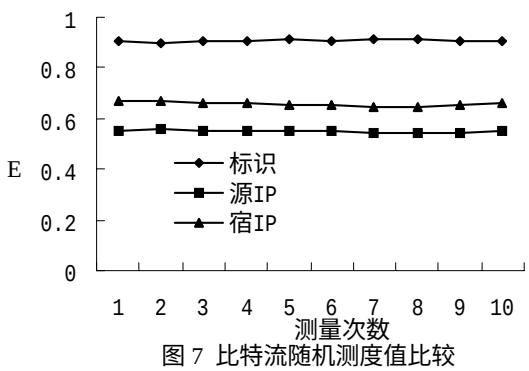

图 7 比特流随机测度值比较

宿 IP 后 16 比特的 E 值比源 IP 后 16 比特的 E 值高出 0.11 左右，表明宿 IP 后 16 比特的随机性比源 IP 后 16 比特的随机性好。分析其原因，我们认为，网络流量由服务器到客户机的流量是由客户机到服务器的流量 3～5 倍

左右，同时网络中服务器的数量远少于客户机，服务器流量集中在少量服务器中，网络流量中服务器 IP 地址的随机性没有客户机 IP 地址的随机性好，故宿 IP 后 16 比特的比特流随机测度值高于源 IP 后 16 比特的比特流随机测度值。

4、抽样测量模型的性能分析

根据上文的分析，确定使用标识字段 16 比特中的部分比特作为抽样掩码匹配位串，理论上使用 0～16 比特的抽样位串，可以实现抽样比率 $1\sim2^{16}$，抽样比率最大可以达 65536 倍。目前普通的 PC 机有 10Mbps 的流量处理和存储的能力，因此使用该模型理论上它最大能抽样测量 640Gbps 的流量，对于目前 CERNET 国家主干 2.5Gbps 和国际上有 40Gbps 的链路完全具有监测能力，当然前提条件是测量器需要具有足够的测量能力。由于抽样模型计算主要是比特运算，便于硬件实现，容易在网卡中实现抽样功能，使得抽样过程不需要主机参与，可以加大测量能力。下面将从抽样模型的随机性和抽样样本统计属性两方面分析抽样掩码匹配测量模型的性能。

4.1 抽样模型随机性分析

标识字段抽样模型的偏移值是一个固定值，定义为标识字段头的位置，即 IP 报头的第 33 比特。其抽样掩码匹配字段长度极限是 16 比特，即选择 IP 报头的第 33 至第 48 之间的比特。首先我们分析从 33 比特至 48 比特之间比特流随机测度值的变化情况。图 8 是测量 10,000,000 个报文标识字段 1～16 比特的比特流随机测度值曲线图，从图中可知，随着抽样掩码比特数的增加，位流熵逐渐减小，但随机测度值最小也能大于 0.9，所以标识字段总体上随机性很大，不同比特之间的相关性很弱。

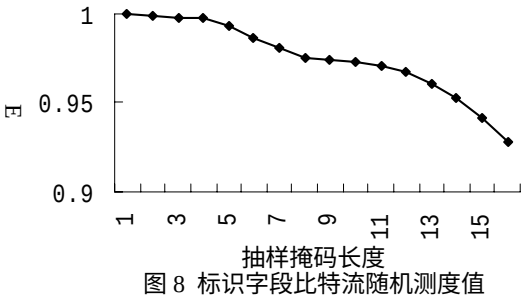

图 8 标识字段比特流随机测度值

图 9 表明抽样掩码长度 n 和抽样比率之间的关系。理论抽样比率 $ratio_t=1/2^n$，对于掩码长度为 n 比特有 2^n 种可能的掩码，对应有 2^n 种抽样比率。图中的 5%、95%、最大值、最小值、中值分别是指 2^n 种抽样比率中分别为 5%、95%、100%、最小值、50%百分位的抽样比率。图 9 可知，中值、95%、5%、最小值的抽样比率几乎和理论抽样比率完全重合。当抽样掩码大于 7 位以后，抽样比率最大值几乎不在变化，通过研究发现是由于抽样掩码全为 0 时的抽样比率远远高于理论值，可能是由于大多应用程序报文的标识字段从 0 开始赋值。因此在设置抽样掩码时，尽量不要采用掩码全 0。图 9 再次证明标识 ID 字段作为掩码匹配字段具有非常良好的随机性能。

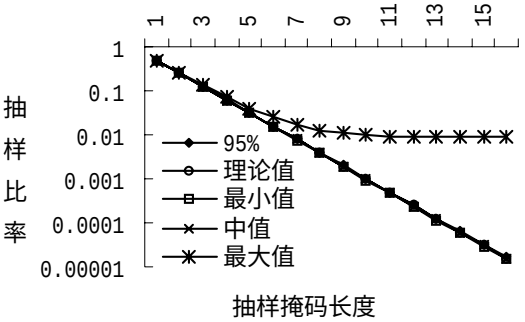

图 9：模型抽样比率关系图

4.2 抽样样本统计属性分析

选定标识字段作为抽样掩码匹配位串，还需要检验抽样样本同流量统计属性的相互独立性，即抽样样本统计（如：报文长度、IP 地址、协议等）应该同流量总体独立同分布。假设总体统计分布函数为 $F_0(x)$，抽样样本统计分布函数为 $F(x)$，检验假设 $H_0:F(x)=F_0(x)$。下面使用皮尔逊 χ^2 检验法[11]对抽样样本和总体进行统计性独立假设检验。

具体方法如下：把样本测量值 $x=(x_1,x_2,\cdots,x_n)$出现的范围划分为 m 组：(c_0,c_1)，(c_1,c_2),…，(c_{m-1},c_m),范围划分考虑分组的统计属性，如源 IP 地址、报文长度及协议，将流量总体属性根据取值范围划分为 I 个箱，如果有 n_i个报文落入第 i 个箱中，那么报文的总数 $n=\sum_{i=1}^{I} n_i$。在抽样样本中，假设有 m_i 个报文落入第 i 个箱中，抽样报文的总数为 $m=\sum_{i=1}^{I} m_i$。因此，在第 i 个箱中有 $u_i=n_i-m_i$个报文没有被抽样，总共没有被抽样测量的报文数是 u=n-m。构造 χ^2分布统计量表示为：

$$\chi^2=\sum_{i=0}^{I-1}\frac{(m_i-n_i p)}{n_i p}\sim\chi^2(I-1) \qquad (4)$$

其中：p 为抽样掩码对应的抽样比率，n_ip 为第 i 箱中抽样样本的理论频数,$n_ip=n_i\times m/n$。对于一个给定的置信系数 1-α（如：α＝5%），如果 $\chi^2<\chi^2_\alpha$，那么认为服从自由度为 I-1 的 χ^2分布，即抽样样本的统计分布和总体的统计分布相同。下面分别就 3 种不同的流量统计属性（源 IP 地址前缀、报文长度、协议）验证独立同分布假设。检验时分别依次使用标识字段 1～16 比特作为抽样掩码匹配位串，实验使用的报文是 10,000,000，抽样掩码分别为：1、10、101、0110、10111、101011、1010111 、 10100100 、 110011101 、1010111000、11110000111、000011110000、1010101010101 、 10000001110010 、011000101110000、0010101011101101，各掩码对应的匹配位串分别为标识字段第 1 位、1-2 位、1-3 位、1-4 位、1-5 位、1-6 位、1-7 位、1-8 位、1-9 位、1-10 位、1-11 位、1-12 位、1-13 位、1-14 位、1-15 位和 1-16 位。

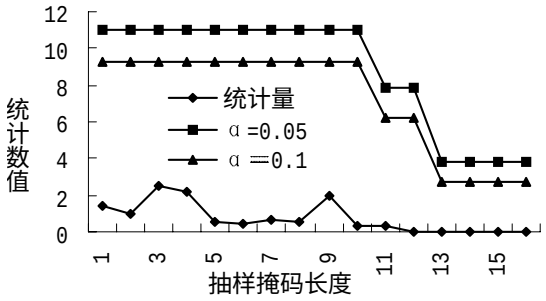

图 10：协议假设检验分布

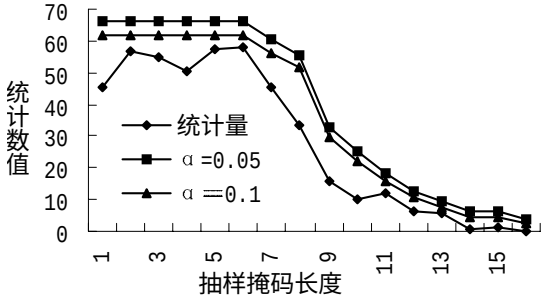

图 11：分组长度假设检验分布

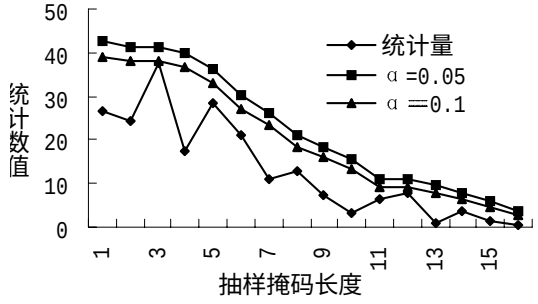

图 12： 源地址前缀假设检验分布

在实验中，验证源 IP 地址前 5 位的分布，使用 $I=2^5$个箱。报文长度集中在 40 字节～1500 字节之间，按每 30 个字节长度设一个箱，因此共设 49 个箱。根据前文分析可知，报文协议类型主要为 TCP、UDP、以及其它类型，可以分成 3 个箱，分别对应 TCP 箱(m_0)、UDP 箱(m_1)和其它协议箱(m_2)，由于报文协议分箱较少，因此，将没有被抽样报文所属的箱 u_0、u_1、u_2也考虑假设检验，故共有 6 个箱。为避免估计误差较大，在假设检验过程中如果 i 箱中频数 np_i小于 5，则将不同的箱加以合并。相关的假设检验分别见图 10：协议假设检验分布，图 11：报文长度假设检验分布，图 12：源 IP 地址前缀假设检验分布。从图中可知，0.05 和 0.01 显著水平检验，均能保证 $\chi^2<\chi^2_\alpha$，故可以

接受 H_0，认为抽样样本的统计属性分布均符合流量总体的统计属性分布，证明基于标识匹配字段的抽样掩码测量模型在统计上是稳定的。

5、结论

抽样测量是目前高速网络研究的热点问题，文章提出一种基于报文内容的抽样测量模型，该模型使用一个抽样掩码匹配报文中某些固定的比特来实现抽样测量，这种抽样测量机制使得抽样算法可以应用于分布式测量环境中。为了描述抽样模型的随机性，文章定义比特随机测度和比特流随机测度量化 IP 报头的随机性，使用这两个随机测度评价通过 CERNET 主干某一路由器流量，发现 IP 报文头的标识字段 16 位可以作为抽样掩码匹配位串。并使用标识字段作为匹配位串的抽样模型对抽样样本的随机性以及抽样样本统计属性的独立性研究表明抽样模型效果显著。

标识字段 16 比特作为抽样掩码匹配位串具有以下优点：1、标识字段在传输过程中不会发生内容变化。2、其位熵和位流熵远高于所有 IP 头的其它各字段，比特随机测度值高达 99％以上，16 位的比特流随机测度值也达到 90％以上，因此，其随机性相当显著。3、由于标识字段是主机判断新来的分段属于哪个分组，是随机产生的一个标记，它不包含报文统计属性相关信息（如：报文长度，IP 地址等），能保证抽样样本在统计属性上的独立性。如果选用其它和统计特性相关的字段（如：报文长度、IP 字段等）或分组内容比特串，将不能保证抽样样本统计上的独立性。4、标识字段长度 16 比特，按目前和未来网络带宽的发展要求，16 比特抽样掩码长度足够使用，这样为各测量器配置抽样信息相当简单，只要确定抽样掩码，而不需要确定偏移和各偏移对应的掩码等多个信息，大大减轻网络传输负担。5、由于标识字段 16 比特连续，不需要对各比特拼装来获取抽样掩码匹配位串，确定函数 H 算法简单，大大加快抽样模型的速度。6、掩码匹配抽样模型只是位运算，便于硬件实现。标识字段的这些优点同其被定义的功能特点相关，IPv6 定义的流标识字段和 IPv4 标识字段功能有相似之处，因此，流标识字段可以考虑作为 IPv6 抽样掩码匹配字段，但这还需要对将来的 IPv6 报文统计分析才能确定。

PSAMP[12]工作组建议抽样测量模型要简单，同时又能满足基于被动测量的各种应用需求。文章提出的抽样测量模型不仅算法简单且测量样本的随机性在统计范围内满足理论值，因此该抽样模型测量不但可用于分布式测量环境，也适用于集中式测量环境，其抽样样本不仅可用于研究网络行为，同时可以直接用于研究流量行为，并能用于网络性能实时监控、实时网络管理以及网络安全入侵检测等应用研究领域。

参考文献

[1] Kevin Thompson, Gregory J. Miller, Rick Wilder. Wide-area Internet traffic patterns and characteristics. IEEE Network, Nov/Dec 1997, Vol. 11 No. 6: 10-23.

[2] I. D. Graham, S. F. Donnelly, S. Martin, J. Martens, J. G. Cleary. Nonintrusive and accurate measurement of unidirectional delay and delay variation on the Internet. In: Proc. INET '98, Geneva Switzerland, Jul. 1998, 21-24.

[3] B. Huffaker, Marina Fomenkov, David Moore, Evi Nemeth, K. Claffy. Measurements of the Internet topology in Asia- pacific Region. In: Proceedings of Inet '00. Yokohama Japan, 2000.

[4] Tanja Zseby, Sebastian Zander, Georg Carle. Evaluation of build blocks for passive one-way-delay measurements. In: Proceedings of Passive and Active Measurement Workshop (PAM 2001), Amsterdam The Netherlands, April 23-24, 2001.

[5] Nick Duffield, Matthias Grossglauser. Trajectory sampling for direct traffic observation. IEEE/ACM

Transactions on Networking, June 2001, Vol. 9, No. 3: 280-292.
[6] I. Cozzani, S. Giordano. A passive test and measurement system: traffic sampling for QoS evaluation. In: GLOBECOM 1998. Sidney Australia, 1998, 1236 –1241.
[7] K. Claffy, G. Polyzos, H. Braun. Application of sampling methodologies to network traffic characterization. In: Proceedings of ACM SIGCOMM '93, San Francisco California, May 1993, 194 - 203.
[8] V. Paxson, G. Almes, J. Mahdavi, M. Mathis. Framework for IP performance metrics. IETF RFC 2330, 1998.
[9] 金振玉. 信息论. 北京: 北京理工大学出版社, 1991.12.
[10] J. Reynolds, J. Postel. Assigned numbers. IETF RFC1700, October 1994.
[11] 唐象能, 戴俭华. 数理统计. 北京: 机械工业出版社, 1994.5.
[12] Nick Duffield. A framework for passive packet measurement. IETF draft-ietf-psamp-framework-00, 2002.

[9] Jin Zhenyu. Information theory. BeiJing: BeiJing University of Science and Technology Press, 1991.12. (in Chinese)
[11] Tang Xiangneng, Dai Jianhua. Mathematics statistics. BeiJing: Mechanism Technology Press, 1994.5 (in Chinese)

Distributed Sampling Measurement Model in a High Speed Network Based on Statistical Analysis

CHENG Guang, GONG Jian, DING Wei
（Department of Computer Science & Engineering, Southeast University, Nanjing 210096）
(Key Lab of Computer Network Technology Jiangsu Province, Nanjing, 210096)

Abstract: The distributed passive measurement is an important technology for network behavior research. But it is very difficult to measure the full trace of high-speed network, so in the paper sampling technology is introduced into network traffic measurement. There are two key technologies that should be solved in the distributed passive measurement. In order to corporate the distributed traffic information, the same packets should be sampled in distributed measurement points. And in order to estimate the statistical attributes of network traffic, the traffic sample should be measured with random. So the key point of the sampling measurement model is to choose some mask bits that can assure the randomicity of the measuring sample and accordant measurement information in distributed measurement points. In the paper, the bit random metrics and bit flow random metrics are defined, and after researching and analyzing huge amounts of packet headers captured randomly on CERNET backbone, the result shows that 16 bits of identification field in IP packet header is enough for matching bits of sampling mask. Randomization and statistical attribute of the sampling are analyzed in the paper, and the experiment also reveals that this sampling way can be used not only in traffic measurement but also for network behavior analysis.

Key Words: sampling measurement, sampling mask, bit entropy, identification field

作者简介：
程光，男，1973 年，博士生，研究方向：网络行为学、网络测量；
龚俭，男，1957 年，博士，教授，研究方向：网络行为学、网络安全；
丁伟，女，1962 年，博士，教授，研究方向：网络管理、网络行为学

CHENG Guang, male, born in 1973, Ph.D student, interested in network behavior and network measurement;
GONG Jian, male, born in 1962, Ph.D, professor, interested in network behavior and network security;
DING Wei, female, born in 1962, Ph.D, professor, interested in network management and network behavior.

联系人：程光
025－3787158（H），
025－3794000－（304）（O）
E-mail: gcheng@njnet.edu.cn