基于分组标识的网络流量抽样测量模型✍

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：PSAMP 建议流量抽样测量模型简单且能够满足各种测量应用要求，为此，文章提出基于报文标识的流量抽样测量模型。对 CERNET 主干网络流量 IP 报头各字段的进行随机性分析，结果表明标识字段 16 比特统计上满足抽样掩码匹配字段的随机性要求。并提出基于标识字段的多掩码抽样测量算法及其修正算法，实验验证其抽样样本既能满足流量统计行为研究，又能进行网络行为研究。

关键词：分组标识，抽样测量，抽样掩码，位熵

1、 引言

网络的飞速发展，网络行为变得越来越复杂，网络行为研究成为网络研究的重点[1]。网络测量是研究网络行为规律的基础，其包括主动测量和被动测量。主动测量在测量过程中向网络注入测试流量，是一种干扰性测量方法，测试流量产生的附加荷载会影响网络链路、路由器的性能状况，最终可能影响测量结果。被动测量直接利用网络中已有的流量，是一种非干扰性测量方法，但它面临高速流量荷载问题，难以实现流量实时测量和处理。被动测量研究主要应用于流量统计行为[1]和网络性能行为[2, 3]研究。

Claffy[4]将被动测量技术用于测量 NSFNET 主干流量的统计行为。Cozzani [5]使用校验和字段模式匹配抽样 ATM 流量，用于研究 ATM 网络的端至端 QoS。Duffield [6]使用哈希抽样算法用于研究路由行为。IETF 工作组分组抽样测量工作组（PSAMP）[7]建议流量抽样测量模型简单且能够满足各种测量应用要求。目前被动测量主要用于两个领域：流量行为分析和网络行为分析，流量行为分析要求保证测量样本的随机性，而网络行为分析要求不同测点测量样本的一致性。为此，文章通过对 CERNET 主干链路的数亿个 IP 报文的统计分析，发现报文标识字段各比特具有很高的随机且独立同分布，并提出基于报文标识的多掩码抽样测量模型，该模型能保证抽样样本统计上的随机性，又能保证测量点之间的一致性。

文章首先描述抽样测量模型，对报文标识字段的随机性和其它报文串随机性进行比较，研究表明标识字段具有足够的随机性满足抽样测量。在验证标识字段随机性基础上提出多掩码抽样测量模型及其修正模型，并对抽样样本的随机性同随机模型进行分析，最后总结全文。

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，先引入评价随机性的测度标准。熵[8]是信息论中的基本概念，用于评价各种随机试验不确定程度，文章将熵的概念推广应用于研究比特随机性。

定义 1，位熵，是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，

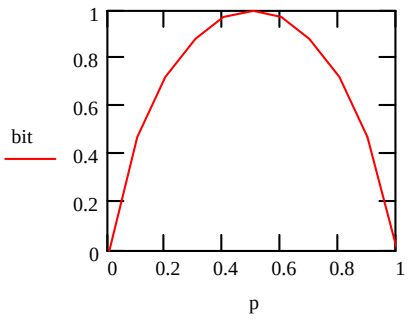

图 1 位熵的变化曲线

✍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

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。比特 b 中 0、1 事件以等概率出现，即当 $p_0 = p_1 = 1/2$，其位熵最大，最大位熵 $H_{\max}(b) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}) = 1$。图 1 位熵变化曲线反映定理 1 的情况。

定义 2，比特随机测度 E，位熵 H（b）和最大位熵 H_{max}（b）的比值，表示比特随机程度的测度，$E = H(b)/H_{\max}(b)$。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 位流熵是比特串所表示的信息量，比特串 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：$H(s) = -\sum_{i=0}^{2^s-1} p_i \log_2 p_i$。　　（2）

定理 2：最大位流熵定理：比特串 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，其位流熵为最大，有 $H_{\max}(s) = -\sum_{i=0}^{2^s-1}\frac{1}{2^s}\log_2\frac{1}{2^s} = s$。　　（3）

定义 4：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，$E = H(s)/H_{\max}(s) = H(s)/s$。

2.2 抽样测量模型

根据 PSAMP 的建议，抽样测量模型要求简单且能够满足各种测量应用要求，使得抽样流量能用于网络流量行为和性能行为研究，流量行为要求抽样流量具有统计随机性，而性能行为要求多点能测量相同的流量样本。为此，文章寻找基于报文内容的抽样测量模型，其核心是确定合适的抽样掩码匹配位串，使得抽样样本能满足网络行为学研究要求。

基于抽样样本的流量行为分析是抽取流量子集以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。基于网络性能行为分析是在不同的测量点能从大规模流量中抽取同样的流量子集，通过研究不同测点流量子集的行为研究网络行为。抽样测量算法需要保证不同测点测量流量子集的一致性，即：网络中的报文要么被其通过的所有测点测量，要么没有测点测量该报文。

如果以报文中某些不变比特串作为流量抽样的激发机制，则能保证测量样本的一致性；如果保证这些不变的比特串在统计上的随机性，则实现样本的统计随机性。那么以这些比特串作为测量模型的抽样掩码匹配的比特串，则抽样样本能够满足流量行为分析和性能行为分析，图 2 为抽样掩码匹配的测量模型。假设被匹配的比特出现 0 和 1 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 $ratio=1/2^n$。被匹配比特必须满足以下几方面因素：（1）传输过程中不发生变化，保证抽样测量样本一致性；（2）具有高随机性，保证测量样本随机性；（3）尽可能与报文统计属性无关。

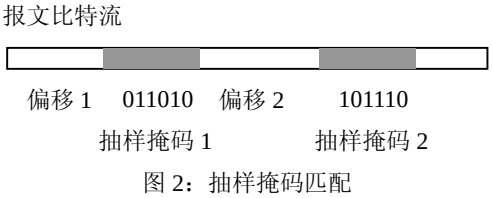

图 2：抽样掩码匹配

比特随机测度和比特流随机测度是描述比特随机性的量化指标，下面将对通过 CERNET

国家主干报文比特的比特随机测度进行分析，选取测度值最大的比特作为匹配比特串，并根据抽样精度确定匹配比特的取值范围。

3、流量比特统计分析

3.1 IP 报头比特随机性分析

文章以千兆光纤网卡、PIII 1G CPU、Red Hat6.2 操作系统，开发直接测量 CERNET 主干链路的测量器，并对 10^8 个 IP 报文头前 20 个字节、160 比特的比特流统计分析。

版本号字段记录报文的版本协议，目前测量的所有报文均为 IPv4，同时报文长度字段几乎均为 5，因此这两个字段的各比特随机测度值 E=0。服务类型字段 8 位中仅有小于 3%的报文使用了这些比特，因此其比特随机性很低。报文长度集中在 40、552、576 和 1500 字节，由于最大长度 1500 字节的限制，其随机测度值较小，且传输过程中可能发生变化。Flag 字段中，88.7%的报文标识 DF 位。0.31%的报文标志 MF 位。offset 字段的比特随机测度值在 0.02 左右，且传输过程中可能发生变化。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，不适合考虑作为匹配比特串。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 占 93.04%，UDP 占 6.37%，其它占 0.59%，因此，协议字段的随机性较小。头校验和每通过一个路由器都发生变化，所有这些均不适合作为匹配比特串。

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 3 是标识字段的比特随机测度值图。标识字段中的 16 位比特随机测度值均在 99%以上，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。

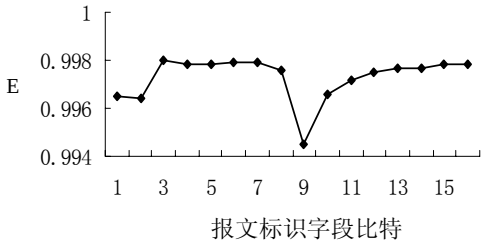

图 3 标识字段比特随机测度值

源 IP 和宿 IP 在传输过程中不发生变化，图 4 是 IP 字段比特随机测度值图。从图可知，IP 字段前 16 比特位熵效率较低，变化幅度较大，而后 16 位字节变化幅度不大，其比特随机测度值达到 90%以上，源/宿 IP 字段在传输过程中不发生变化，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。

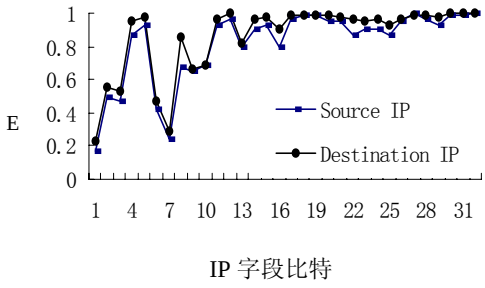

图 4 IP 字段比特随机测度

3.2 位流熵分析

根据以上对 IP 报头各字段的随机性统计分析，标识字段、源/宿 IP 后 16 比特具有传输过程不变且比特随机测度值大，初步选定这 3 个位串可以作为抽样掩码匹配位串，下面将分析这 3 段 16 比特串中各比特之间的相关关系。

文章从 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 10^7 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，其结果见图 6。其中标识字段 16 比特流随机测度值远大于其它值，因此使用标识字段作为匹配比特串能保

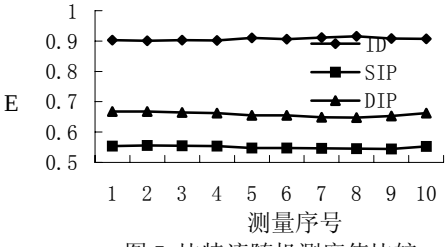

图 5 比特流随机测度值比较

证抽样样本的统计随机性。

4、标识字段的随机性及其修正

根据上文的分析，确定使用标识字段可作为被匹配比特串，理论上使用 0～16 比特的抽样位串，可以实现抽样比率 1～2^{16}，抽样比率最大可以达 65536 倍。下面将从抽样模型的随机性分析抽样测量模型的性能。图 6 是测量 10^7 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，随着抽样匹配比特串长度的增加，随机测度值逐渐减小，但最小值也能大于 90%以上，所以标识字段各比特之间的相关性很小。图 7 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 $ratio_t=1/2^n$，n 比特有 2^n 种可能的掩码，对应有 2^n 种实际抽样比率。图 7 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%百分位数初的抽样比率。图 9 可知，中值、95%、5%、最小值的抽样比率和理论抽样比率几乎完全重合。而当抽样掩码长度大于 7 位以后，抽样比率的最大值几乎不再减少，研究表明由于抽样掩码全为 0 时的抽样比率远远高于理论抽样比率，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。

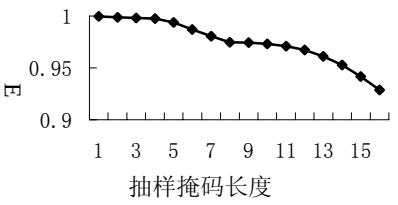

图 6 标识字段比特流随机测度值

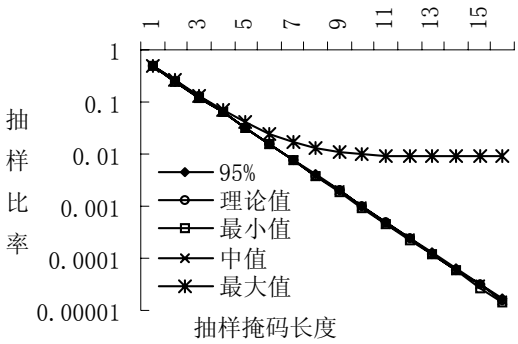

图 7：模型抽样比率关系图

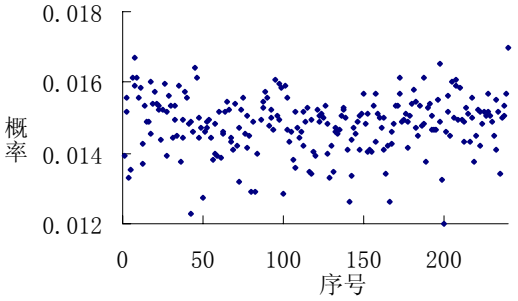

图 8 标识字段 0 值概率散列图

图 7 表明随着匹配掩码长度的增加，比特流随机测度值下降。研究发现标识字段值为 0 的概率远大于其理论概率值，图 8 为测量时间粒度为 5s，标识字段 0 出现概率的散列图。图 8 表明标识字段 0 的概率为 1.4%～1.6%之间，远大于理论概率 1/65536 的抽样概率。

设标识字段 0 的报文总数为 count0，总报文为 countfull，理论标识字段 0 的报文总数为 count0_theory，则多余的标识字段为 0 的数目为 count0-count0_theory，除多余标识字段 0 的数目，理论总报文数为 count_theory=countfull-(count0-count0_theory)，而 count0_theory=count_theory*1/65536，因此理论报文总数为 count_theory = (countfull-count0)×65536/65535。则标识字段 65536 种事件出现的次数除以 count_theory 为该事件的修正概率，根据修正概率计算的比特流随机测度值为修正随机值。标识 0 修正之前和修正之后其随机测度值的变化见图 9，每次测量 10^6 个报文。同修正前 95%随机测度值相比，经过修正的标识字段流随机测度值达到 99%，且波动更小。

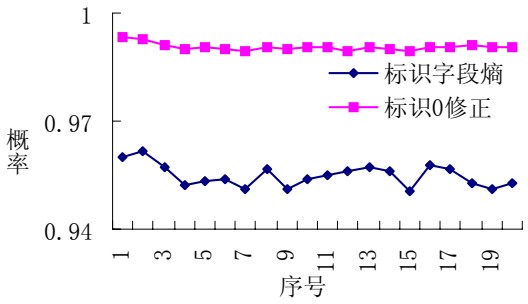

图 9 标识字段随机测度值曲线

5、基于标识字段的多掩码抽样测量模型

5.1 多掩码抽样测量模型描述

上文研究标识字段的随机性，下面将着重研究基于标识字段的抽样算法，前文描述掩码法定义一串字符串作为掩码 M，掩码长度 L，如果标识字段的指定比特串同掩码 M 匹配，则抽样该报文，否则丢弃报文。理论上，长度 L 的掩码抽样的比率为 $1/2^L$。掩码法的缺点是其控制的抽样比率范围很小，长度为 16 比特的标识字段仅有 16 种抽样比率，分别为 1/2、$1/2^2$、$1/2^3$、$1/2^4$、$1/2^5$、$1/2^6$、$1/2^7$、$1/2^8$、$1/2^9$、$1/2^{10}$、$1/2^{11}$、$1/2^{12}$、$1/2^{13}$、$1/2^{14}$、$1/2^{15}$、$1/2^{16}$。这 16 种抽样比率无法描述实际测量需求，为此文章提出将不同抽样掩码组合以实现任意抽样比率，即 3/8 的抽样比率，可以定义 $1/2^2$ 和 $1/2^3$ 两种抽样掩码。

上文已经证实标识字段的比特随机分布，各事件出现的概率在统计范围内服从等概率分布。使用多个抽样掩码，使得不同抽样掩码对应的抽样比率能够直接叠加，必须保证不同的抽样掩码之间独立不相关。设 n 个抽样掩码（a_i : i = 1 to n）的长度分别为 L_i: i = 1 to n，其对应的抽样比率分别为 $1/2^{L_i}$，则使用这 n 个抽样掩码的抽样概率为 $ratio = f(\sum_{i=1}^{n} 1/2^{L_i})$，如果这 n 个掩码之间是独立不相关，则抽样概率为 $ratio = f(\sum_{i=1}^{n} 1/2^{L_i}) = \sum_{i=1}^{n} 1/2^{L_i}$ 。

因此首先要定义一种抽样掩码定义规则，保证不同的抽样掩码之间独立不相关，同时抽样掩码定义还应该满足条件（1）匹配时间复杂度小；（2）不同服务器之间需要确定的抽样掩码参数；（3）尽可能满足抽样报文的标识字段在所有标识字段中分布均匀、随机。为此抽样掩码的定义规则为：

（1）抽样掩码第 1 个比特对应标识字段第 1 个比特，即偏移为 0；

（2）长度为 L 的抽样掩码，其前面 L-1 个比特取值为 0，第 L 个比特取值为 1

根据以上规则，抽样参数定义为：设 n 个抽样掩码长度分别为 L_i: i = 1 to n，其掩码值定义为子掩码的抽样参数，即如果子抽样掩码长度为 L_i，则根据抽样掩码定义规则，其子抽样参数 parameter = 2^{L_i} 。同时，知道抽样参数，可以将其转化为用 2 进制表示的抽样掩码。因此根据上面规则，n 个子抽样掩码的参数定义为 parameter= $\sum_{i=1}^{n} 2^{L_i}$ 。由于任何整数可以用多个不同的 2^i 组合得到，因此可以通过对 parameter 进行 2 幂分解得到各个抽样掩码的抽样参数，任何抽样参数可以转化为抽样掩码。下面给出多掩码抽样算法及其参数转化算法。

5.2 多掩码抽样算法

任意抽样比率 ratio∈(0, 1)，使用以下抽样比率分解算法将其转化为多个子抽样掩码：

设抽样参数为 parameter=0;

for i from 1 to 16

{ if ratio >= $1/2^i$ then

ratio = ratio – $1/2^i$

parameter = parameter + 2^i

end if }

return parameter

抽样比率分解算法可以保证抽样比率可以在 16 次循环之内转化为抽样参数，其抽样精

度可控制在 1/65536 范围之内，相对精度误差为 1/65536*ratio。测量器得到抽样参数以后，可以使用以下参数分解算法将参数分解为对应的抽样掩码长度。

设抽样掩码参数存放数组为 mask[ ] = 0;

抽样掩码个数 number = 0;

for i from 1 to 16

{ if parameter > = 2^i then

mask[number] = i

number ++;

end if }

return number, mask[ ]

知道抽样掩码长度，根据抽样掩码定义规则，即可知道对应的抽样掩码。对于到达的报文，根据由以下的抽样算法决定是否抽样报文：

设到达报文的标识字段第一个出现非零的位置是第 L 个比特；

bool sampling = 0; //如果 sampling 为 0 表示该报文不抽取，否则表示抽样该报文。

for i from 0 to number – 1

{ if mask[i] = = L then

sampling = 1

return sampling

end if }

return sampling

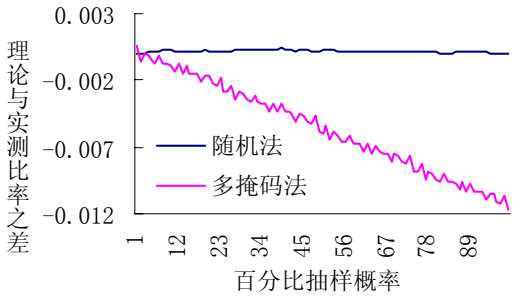

图 10 随机模型和多掩码模型关系

下面举例分析各算法，设要求抽样比率为 0.638，根据抽样比率分解算法将 0.638 分解为：0.638=$1/2^1$+$1/2^3$+$1/2^7$+$1/2^8$+$1/2^{10}$+$1/2^{12}$+$1/2^{15}$+ $1/2^{16}$+0.0000148 。相应的抽样参数 parameter = 2 + 2^3 + 2^7 +2^8 +2^{10} +2^{12} +2^{15} +2^{16} = 103818。分析器可以将抽样参数 103818 传送到测量器，测量器根据抽样参数分解算法将抽样参数分解成子掩码长度，其 number = 8，抽样掩码位置数组为 mask() = {1, 3, 7, 8, 10, 12, 15, 16}，其对应的各子抽样掩码分别为 1、001、0000001、00000001、0000000001、000000000001、0000000000000001、0000000000000001。最后根据抽样算法抽样测量到达的报文。其中抽样比率分解算法和抽样参数分解算法为测量之前的任务，而抽样算法为测量过程中使用的算法。

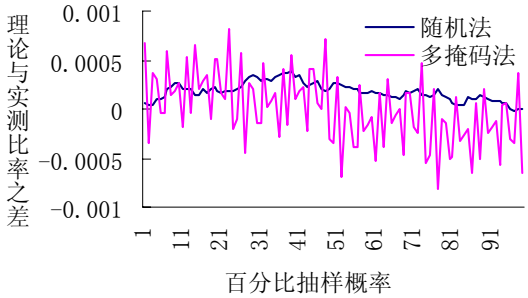

图 11 随机模型和修正多掩码模型

5.3 多掩码算法和修正多掩码算法的比较

图 10 为测量 10^7 个报文抽样概率 1%～99%的多掩码抽样概率和随机抽样概率和理论抽样概率的差值关系，从图 8 可知，由于标识字段 0 出现的概率超出理论概率，因而随着抽样概率的增大，其多掩码抽样概率误差也随之增大。图 11 为根据第 4 节修正标识 0 后的理论概率和抽样概率之间的误差图，修正后的模型精度明显高于修正前精度，其估计误差集中在-0.05%～+0.05 之间。

6、结论

抽样测量是目前高速网络研究的热点问题，文章提出基于报文标识字段的抽样测量模型，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。通过 CERNET 主干某一路由器流量的分析，发现 IP 报文头的标识字段 16 位可以作为匹配比特串，并分析抽样样本的随机性，研究表明抽样模型效果显著。

为了能够测量任意的抽样比率，文章提出的基于标识字段的多掩码抽样测量模型，并研究抽样模型的修正模型，将抽样模型同随机法比较结果表明，修正的多掩码抽样测量模型的随机程度接近随机算法产生的随机性。研究表明基于标识字段的多掩码修正抽样测量的测量样本即可用于网络流量行为研究，也可用于网络性能行为研究。

参考文献

[1] Kevin Thompson, Gregory J. Miller, Rick Wilder. Wide-area Internet traffic patterns and characteristics [J]. 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 [C]. Proc. INET '98, Geneva Switzerland, Jul. 1998, 21-24.

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

[4] K. Claffy, G. Polyzos, H. Braun. Application of sampling methodologies to network traffic characterization [C]. Proceedings of ACM SIGCOMM '93, San Francisco California, May 1993, 194 - 203.

[5] I. Cozzani, S. Giordano. A passive test and measurement system: traffic sampling for QoS evaluation [C]. GLOBECOM 1998. Sidney Australia, 1998, 1236 –1241.

[6] Nick Duffield, Matthias Grossglauser. Trajectory sampling for direct traffic observation [J]. IEEE/ACM Transactions on Networking, June 2001, Vol. 9, No. 3: 280-292.

[7] Nick Duffield. A framework for passive packet measurement [S]. IETF draft-ietf-psamp-framework-00, 2002.

[8] 金振玉. 信息论 [M]. 北京: 北京理工大学出版社, 1991.12.

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，博导，研究方向：网络行为学、网络安全；

Network traffic Sampling Measurement Model on Packet Identification

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: A new sampling model for measurement using packet identification on IP network is provided in this paper under a principle of PSAMP, a working group of IETF, that a good sampling model should work for all purposes of measurement applications at the same time with a simple way. 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. Then a multi-mask sampling measurement model on identification and its corrected model are provided 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: Packet Identification, Sampling Measurement, Sampling Mask, Bit Entropy