大规模网络流量分组标识方法的分析研究[1]

赵钧　程光　丁伟

（东南大学计算机科学与工程系　南京 210096）

摘要：分布式被动测量技术的核心问题之一是分组标识的生成方法。文章对生成分组标识的基本原则和方法进行了分析和研究，并使用除留余数法、MD5 和折叠法三种分组标识生成算法对 CERNET 主干的流量进行实验，分析冲突率和分组标识长度之间的关系。研究结果对被动测量应用具有重要意义。

关键字：被动测量，分组标识，散列，冲突率

中图分类号：TP393　　**文献标识码：**A

1 引言

近年来，网络行为学的研究成为热点。掌握网络行为的基本特征有助于网络规划、网络管理、网络安全和新网络协议及应用的设计等研究工作的进行。而网络行为的测量和分析则是网络行为学研究的基础。

目前网络测量根据网络行为研究方向大体可分为拓扑测量、流量性能测量和端至端性能测量。网络的测量方法[1]主要有主动测量和被动测量两种。主动测量通过向网络中发送测量流量来获取两指定端点间的网络性能的信息。被动测量则是在网络中某一点监听经过的报文，以获取网络的流量信息。这两种测量方法各有优缺点，适用于不同的场合。主动测量可以获取端至端的网络性能信息，但是由于需要向网络发送流量，必然会对网络的性能产生影响，从而使测量值偏离实际值。也就是说，这种方法有着天然的系统误差。相比而言，被动测量不影响网络本身的运行情况，可以获得客观的数据。但是被动测量目前主要用于单点获取数据，难以进行网络行为分析，如路由分析[2]、端至端行为分析[3, 4]等。

如果能将被动测量方法应用于端至端的性能分析，则可以避免主动测量带来的系统误差。在两个使用被动测量方法的监测点之间进行端至端的性能分析，关键是对经过这两个监测点的报文进行识别，也就是说，如果某报文经过监测点 A，则其在经过监测点 B 时，也能被识别出来。这样，这个报文就起到了主动测量中的测量报文的作用，从而可以进行端至端的性能分析。

文章首先介绍在被动测量条件下对报文进行识别的原则性方法。然后用三种散列方法对报头中的若干字段进行处理，生成报文标识，并对其进行实验比较。最后给出结论。

2 标识的生成方法

为了能使不同的测量点对同一报文产生相同的标识，必须选用报文在传输过程中不发生变化的字段。而为了区别不同的报文，则应该选用报文之间差别很大的字段。

对于 IP 报文，报文的数据内容千差万别且没有结构性，报文之间没有可比性，因而不适于用来生成标识。而报文的控制字段，即报头是结构化的数据，各个字段都有确定的语义，不同的报文的相同字段可以比较、区分，进而能唯一识别标识一个报文。但是，并不是报头中的所有字段都满足上述原则性要求的。比如，IP 报头的版本号（Protocol Version），报头长度（Header Length），服务类型（Type of Service）等字段，各个报文都基本相同；生存时间（Time to Live），报头校验和（Header Checksum）等字段，在传输过程中会发生变化；而协议类型（protocol）字段一共就只有有限的几个值，不同报文之间差别不大。相比而言，IP 报头的源地址、宿地址和 packet ID，以及传输层协议报头的源端口和宿端口这五个字段在传输过程中不发生变化，各个报文之间差异也比较大，满足上述的原则性要求，可以用来识别报文。

以上所选的 5 个字段共有 14 个字节 112 个比特。从通信、存储和处理的开销方面考虑，报文的标识当然是越短越好。因此，需要对这 5 个字段进一步压缩，生成报文标识。

散列技术可以用来压缩信息的长度，同时散列值能够较好地保持不同信息间的差异，因而被用来产生信息摘录，进行数据的完整性保护。本文将使用以下三种散列的方法对以上五个字段进行处理，生成报文

[1]本文受国家 863 项目 2001AA112060 资助。

作者简介：赵钧，男，1974 生，东南大学计算机科学与工程系在读硕士研究生。

的标识。

（1）除留余数法

将这 5 个字段按源地址，宿地址，源端口，宿端口，packet ID 顺序并置，构成一个 112 位的二进制数，然后除以 $2^n - 1$，余数作为标识，其中 n 为标识的比特数[5]。

（2）MD5 法

MD5 算法是标准的信息摘录算法，它以任意长度的字节流为输入，输出 128 比特的信息摘录。MD5 算法在 rfc1321[6]中有详细的介绍。

（3）折叠法

将以上 5 个字段构成源地址，宿地址，端口和 packet ID 四个 32 比特的字，其中端口字由源宿端口并置而成，packet ID 前 16 位用 0 填充。将这四个字进行异或操作，取结果字的后 n 比特作为标识。

以上三种散列方法的计算复杂性，由低到高分别是折叠法，除留余数法，MD5 法。

由于散列算法的输入信息的长度大于输出信息的长度，因此会有不同的输入产生相同的输出的可能，即发生冲突。输出信息（标识）越长，产生冲突的可能性也就越小[7]。因此需要找到一个折中的标识长度 n，它尽可能小，而产生的冲突又在可接受的范围内。

用以上三种散列方法对从网络中心采集到的 100 万个报文进行处理，实验结果分析如下。

3 实验结果与分析

定义冲突率（conf_ratio）为具有相同标识的报文数占报文总数的百分比：

conf_ratio = (same_count / total_count) * 100%

其中，same_count 为具有相同标识的报文数；total_count 为报文总数。

以下用冲突率作为算法性能比较的指标。

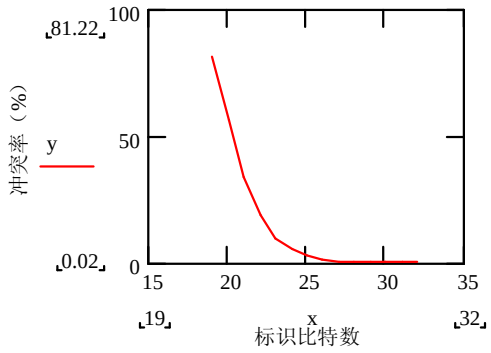

图-1 MD5 法和折叠法冲突率变化趋势

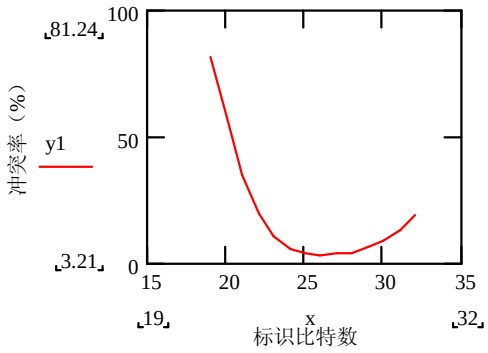

图-2 除留余数法冲突率的变化趋势

实验表明，MD5 方法和折叠法随着标识长度的增加，冲突率下降，但是下降的幅度越来越小（图-1）。而在标识长度相同的条件下，MD5 的冲突率要小于折叠法。

除留余数法开始时也是与 MD5 方法和折叠法以相同的趋势变化，其冲突率介于两者之间。但后来又发生了异常的变化，这和模数的选取有关（图-2）。

定义冲突减小变化率（Δde_ratio）为标识长度为 n － 1 时的冲突率与标识长度为 n 时的冲突率的差值与标识长度为 n 时的冲突率的比：

Δ de_ratio(n) = [conf_ratio(n － 1) － conf_ratio(n)] / conf_ratio(n) * 100%

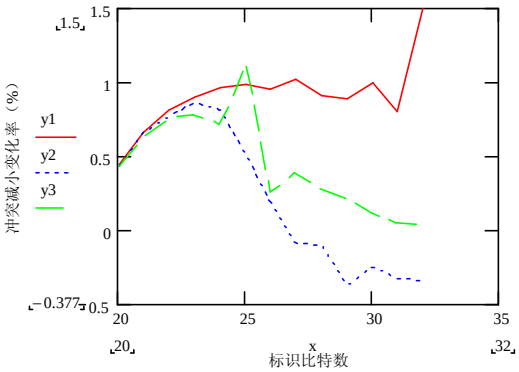

图-3 冲突减小变化率的比较

其中，conf_ratio(n － 1)为标识长度为 n － 1 时的冲突率，conf_ratio(n)为标识长度为 n 时的冲突率。

计算以上三种方法在各点的冲突减小变化率，并将其绘制成图-3。其中，y1 为 MD5 法，y2 为除留余数法，y3 为折叠法。

由图可以看出，随着标识长度的增加，MD5 算法的冲突减小变化率是稳中有升，而除留余数法和折叠法都呈下降的趋势，其中除留余数法下降得更快一些。计算三者的平均冲突减小变化率，MD5 为 0.91%，除留余数法为 0.21%，折叠法为 0.44%。这说明 MD5 算法对标识长度的增加更为敏感，性能提高得更快。

总的来说，MD5 算法的性能最好，折叠法次之，而除留余数法最末。

4 结论

将被动测量技术应用于网络行为分析，这在网络行为测量领域是一个新的思路。这种方法不干扰网络本身的流量，因而测量结果比主动测量技术更为准确、客观，也因此有着良好的应用前景。而其中的关键技术之一就是对报文进行识别。

本文对生成报文标识的基本原则进行了分析和研究，并根据这一原则提出了三种用散列的方法生成标识的算法，同时通过实验对这三种算法的性能进行了比较。MD5 算法在相同的标识长度下，具有最小的冲突率。除留余数法的散列效果与所选取的模数有关，在数据动态变化的条件下，选择一个静态的模数很可能得不到满意的效果。而折叠法计算复杂性最小，适当增长标识长度，也能取得较好的散列效果。因此，在对算法时间要求不高的条件下，可以选用 MD5 算法，它可以以较短的标识满足低冲突率的要求。在高速环境下可以选用折叠法，它速度最快，但需要较长的标识来满足低冲突率的要求。而除留余数法，因其散列效果与所选取的模数有关，一般不予考虑。

参考文献：

[1]程光，龚俭，“大规模高速网络流量测量研究”，计算机工程与应用，2002，Vol 38:5(17-19)

[2]Nick Duffield, Matthias Grossglauser, Trajectory Sampling for Direct Traffic Observation, Proceedings of ACM SIGCOMM 2000, Stockholm, Sweden, August 28 – September 1, 2000

[3]Tanja Zseby, Sebastian Zander, Georg Carle, Evaluation of Build Blocks for Passive One-way-delay Measurements, PAM2001

[4]Ian D. Granham, Stephen F. Donnelly, Stele Martin, Jed Martens, John G. Cleary, Nonintrusive and Accurate Measurement of Unidirectional Delay and Delay Variation on the Internet, INET’98, Geneva, Switzerland, 21-24 July, 1998.

[5]严蔚敏，吴伟民编著，《数据结构》，第二版，清华大学出版社。

6]RFC-1321，R. Rivest，"The MD5-digest Algorithm"，April 1992。

[7]龚俭，陆晟，王倩编著，《计算机网络安全导论》，东南大学出版社。

An Analystic Research on the Method of Generating Packet Identifiers of the Traffic on a Large-scale Network

Zhao Jun　Cheng Guang　Ding Wei

Department of Computer Science and Engineering, Southeast University

Nanjing 210096

Abstract: One of the key point of the technology of distributed passive measurement is the method of generating packet identifiers. In this article, the principles and the methods of generating packet identifiers is analyzed and studied. And three methods, modular, MD5, and folding, are introduced and experimented with the traffic on the CERNET backbone. Within the experiment, the relationship of conflict ratio to the length of the packet identifier is analyzed. The result is of importance to the application of passive measurement.

Keywords: passive measurement, packet identifier, hash, conflict ratio.