TCP 数据流的非对称性分析(修改稿)[1]

戴宣，丁伟，程光

（东南大学计算机系 江苏南京 210096）

（江苏省计算机网络技术重点实验室）

摘　要：本文提出了一个面向TCP流属性的非对称性测度，包括该测度的定义和计算方法。并基于这个测度对CERNET的一个千兆省网边界的实际数据进行了分析。分析工作从流长度（报文数）和流字节数2个属性角度展开，利用一组函数对这些流属性的非对称测度进行了统计和分析，获得了一组有关的结论，可以用于与网络行为学有关的研究。

关键词：TCP 数据流；非对称性；流属性；测度；网络行为学[1]

The Analysis of the Asymmetry of TCP Data Flow

DAI Xuan， DING Wei，CHENG Guang

(Dept. of Computer Science & Engineering, Southeast University, Nanjing 210096)

(Key Lab of Computer Network Technology in Jiangsu Province, Nanjing 210096)

Abstract: An attribute-oriented asymmetric metrics is proposed firstly for TCP flow by the definition and the way of calculation. With which and after being rebuilt to TCP flow, two traces of IP packet sniffed from a gigabyte backbone boundary of CERNET are analyzed on the attributes of TCP flow length (packet number) and flow bytes. Some interesting characters behind the flow are appeared, which can be used for network behavior research.

Keywords: TCP Data Flow; Asymmetry; Flow Attribute; Metrics; Network Behavior

1 引言

在基于 TCP/IP 的互联网环境中，所谓数据流指的是在某条特定信道上传送的符合特定的规范（specification）和超时（timeout）约束的一系列报文的集合[2]。目前，被普遍承认且被广泛使用的数据流规范是将 IP 报文头按（源 IP，宿 IP，源端口，宿端口，协议号）五元组分类，在满足超时约束的条件下，每一类就是一个数据流。还可进一步按照协议类型将流分成 TCP 流和 UDP 流等.

对 UDP 流而言，上述数据流的定义是明确且无二义的，但对 TCP 流来说，情况就要复杂些。从严格的意义上讲，一个完整的 TCP 连接都会产生 2 个方向相反的单向数据流，但它们是相互关联的。因此，可以认为一个 TCP 数据流是由 2 个单向流构成的。

这 2 个单向流在用相同计算定义（函数）产生的属性（测度）值之间会存在一定的差异，这个差异称为 TCP 数据流的非对称性，与之相关的研究就是 TCP 数据流非对称性研究。

从宏观角度看，互联网上的流量存在非对称性，这是一个公认的事实。但目前更进一步、更具体的对于非对称性现象的研究并不多见，常见的 TCP 流研究内容多是对流量突发性及其延时的测量[3]。考虑到网络中的 TCP 流数量占有绝对优势[4]。为此，我们选取了普通 TCP 数据流为切入点，以非对称测度为主要手段，从长度和字节数两个角度进行数据流的非对称性分析。从中寻找普通 TCP 数据流非对称性的一般变化规律和有关特性。

本文研究工作的原始数据来源于一个高速网络测量系统 WATCHER[5]，该系统位于 CERNET 的一个省网边界，它能在千兆信道上，以低的丢包率采集所有 IP 报文头，并依照上述数据流定义进行组流，并进行相关的统计，计算有关的属性和参数。相对于常用的仿真分析而言，这种基于主干信道真实数据的分析所获得的结论更有意义和说服力。

*[1] 本文受国家 973 项目 2003CB314803 资助

作业号	起始时间	中止时间	总流数	TCP 流数	TCP 流所占比例	丢包率
23	7/30/2004 13:50:22	7/30/2004 15:50:22	24927343	18852991	75.6%	3.3%
31	10/21/2004 21:00:00	10/22/2004 09:00:00	82908993	71884341	86.7%	3.4%

表 1 分析用数据的基本情况

本文将在下面的章节中首先详细介绍本文分析所使用的数据来源和有关分析手段的描述定义，然后是对普通 TCP 数据流非对称性变化规律进行的研究和总结。

2.数据来源和有关定义

2.1 数据来源

如上所述，Watcher 是一个可以在实际的互联网主干上，采集 IP 报文头信息（44 个字节），并将其组成数据流的系统。本文所使用的分析数据来源于该系统在 CERNET 的一个省网边界（1G）上的两次实际运行（称为两次作业，或 trace）。所有进出省网的报文都将进过该边界，这将保证得到的数据流的完整性。为避免偶然性并使结果更具普通性，所选择的两次作业在时段和持续时间等基本参数上均有很大不同。两次作业的信息见表 1。

其中的 TCP 流为 TCP 数据流。同时 WATCHER 能给出每个流的长度、字节数等细节参数，对 TCP 数据流还可以分别给出 2 个方向流的各种详细参数。

2.2 数据预处理

根据 TCP 协议的交互特性,一次有效的 TCP 连接从建立连接到断开连接，至少需要六个报文[6]；此外，正常的 TCP 连接中也不可能只含有一个单向流。所以，可以将所含报文数在 6 以下以及只含一个单向流的数据流排除。经过统计，在两次作业中 TCP 数据流所含报文数在 6 以下的流共有 25033991，占 TCP 流总数的 27%；而只在一个单向流上有报文的数据流的个数为 6958096，占 TCP 流总数的 7%。导致上述问题出现的原因可能是多方面的，如安全攻击、超时[2]等，但它们不是本文讨论的问题，因此在下面的讨论中，我们将这些流看作噪声，将其从整体中排除。

2.3 数据流长度和非对称性测度定义

定义 1：一个数据流（单向流）中所包含的报文数称为该流的流长度。

定义 2：设 TCP 数据流 f=（fx，fy），fx 和 fy 为互为对应的、方向相反的单向流。X 为 fx 中流的某种属性值，Y 为 fy 中流的同种属性值，不失一般性，设 X>0，Y>=0，则流 f 关于该属性的非对称性测度 F 为：

$$F(f)=\left|\frac{X-Y}{X+Y}\right|$$

例如，若 X，Y 分别表示流的长度，则 F 就是关于流长度的非对称性测度；若 X，Y 分别表示流的字节数，则 F 就是关于流字节数的非对称性测度。

显然，F 函数具有以下性质：

- $0 \le F \le 1$
- F＝0 当且仅当 X=Y
- F＝1 当且仅当 Y=0，此时，称 f 为单向流
- F→0，表明 f 两个方向上的属性值接近，非对称性弱
- F→1，表明 f 两个方向上的属性值相差较大，非对称性强

由于 F 具有以上性质，因此我们将利用它进行对称性研究分析。

2.4 F 函数分段统计方法和加权平均值

假设所关注的 TCP 数据流属性（长度或字节数）值的上限为 M，将（0，M）等分为 n 个区间，记为 $X_1, X_2, X_3 \cdots X_n$。

定义 3：对于一个任意选定的属性区间 X_i，设落入该区间的 TCP 数据流总数为 N_i，分别记做 $f_1, f_2, \cdots\cdots f_{Ni}$，它们所对应的非对称测度值分别为 $F(f_1), F(f_2), \cdots F(f_{Ni})$，不失一般性，设 $F(f_1)<F(f_2)<\cdots<F(f_{Ni})$，则 F 的百分比函数定义为 $F_{m\%}(X_i)= F(f_{m\%*Ni})$

很显然，这个函数表示在该区间内，有 m%的流

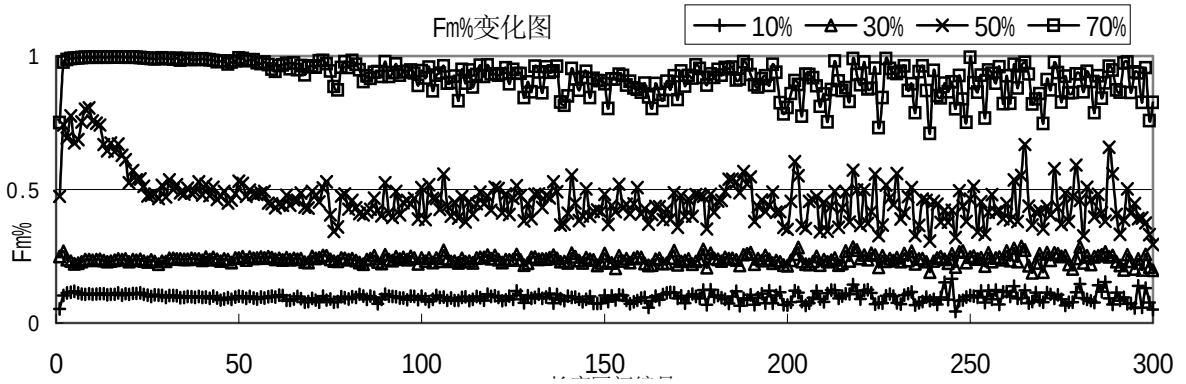

图 1 基于流长度的非对称测度函数 $F_{m\%}$曲线图

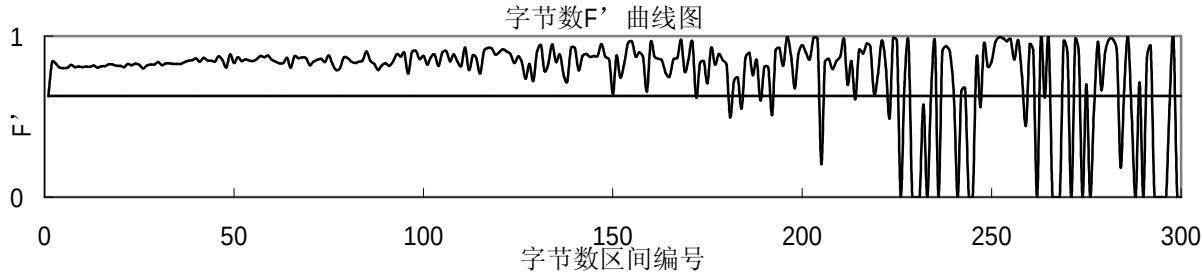

图 2 流长度的加权平均非对称测度函数 F’曲线图

的非对称测度值小于等于该值，而有(1-m%)的流的非对称测度值大于等于该值。

也可以引入加权平均值的方法来比较非对称性。 此时，将 F 函数的值域区间[0,1]等分为 100 个，记为 $Y_1,Y_2,Y_3 \cdots Y_{100}$。对于任意上述区间 X_i，记流长度在区间 X_i 内的数据流个数为 N_i，其 F 值落在区间 $Y_1,Y_2,Y_3 \cdots Y_{100}$ 的流个数分别为 $N_{i1},N_{i2},N_{i3} \cdots N_{i100}$，这样有

定义 4：TCP 数据流某属性基于分段的加权平均非对称测度函数

$$F'(X_i)=\frac{\sum_{i=1}^{100}(j-0.5)*Nij}{Ni*100}$$

该函数反映特定属性值区间内的流的非对称测度的总体非对称性程度。

定义 5：非对称测度函数均值定义为

$$\overline{F}=\frac{\sum_{i=1}^{n}Ni*F'(Xi)}{\sum_{i=1}^{n}Ni}$$

下面将使用定义 3 到定义 5 中给出的函数对第 2 小节中描述的数据进行分析和处理。

3 流长度的非对称性分析

这里流长度参数指一个流中所包含的报文（分组）数。根据 2.1，两次作业一共获得的 TCP 流个数为 90737332。同时根据 2.2 的分析，将所有的 695296 个单向流去掉，最终用于分析的有效的流数量为 90042036 个。根据 WATCHER 提供的长度统计发现这些有效流中 99％的流的长度都在 6－60000 内，因此在本小节的分析中取 M＝60000。之后，取 n＝300，将流长度范围平均分成 300 个区间，为 X 轴上区间编号（1－300）。

分别取 m＝10、30、50 和 70，得到 $F_{m\%}$函数的图形如图 1 所示。

1) 可以看出，超长流（含报文数大于等于 1000）的 $F_{m\%}$值波动较大，长流（含报文数小于 1000 且大于等于 10）和短流（含报文数小于 10）的 $F_{m\%}$值相对平稳。这是因为超长流数量较少，导致出现的超长流随机性较大，使得 $F_{m\%}$值波动较大。统计后发现两次作业所得 TCP 流中，长流和短流一共有 89659891 个，占了 TCP 流总数的 98％。
2) $F_{70\%}$的曲线与 $F_{50\%}$的曲线相比上升幅度较大，其中前者非常接近 1，这个特性在长流区间内表

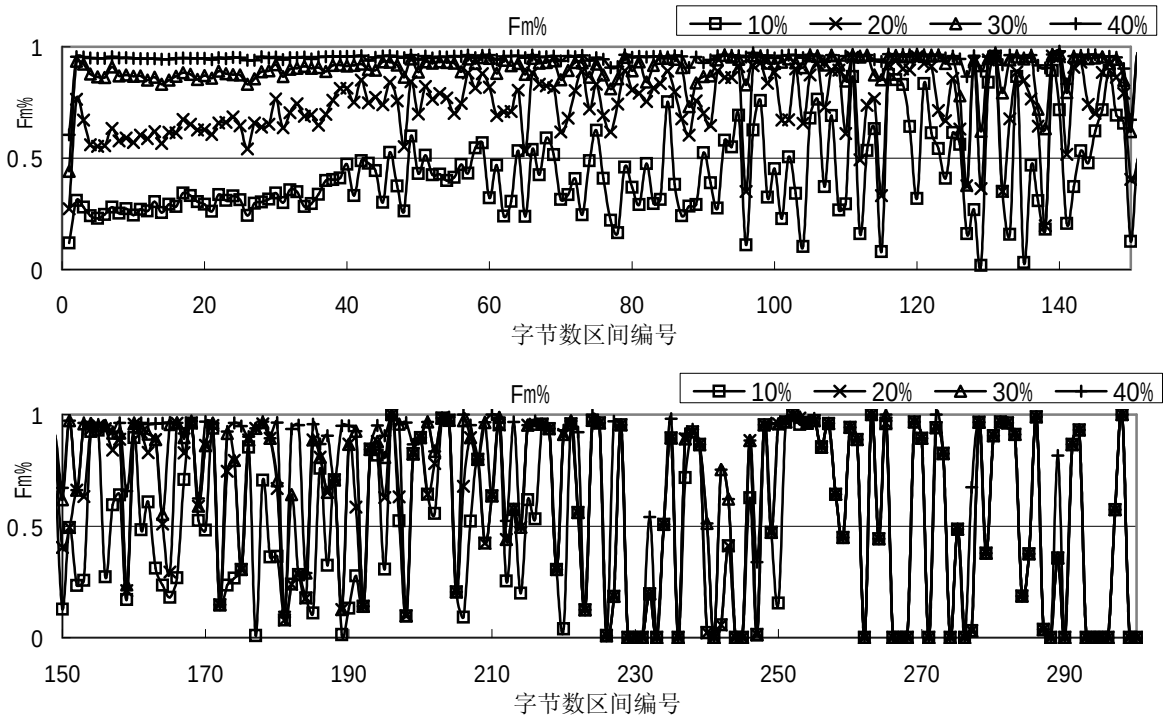

图 3 基于流字节数的非对称测度函数 $F_{m\%}$曲线图

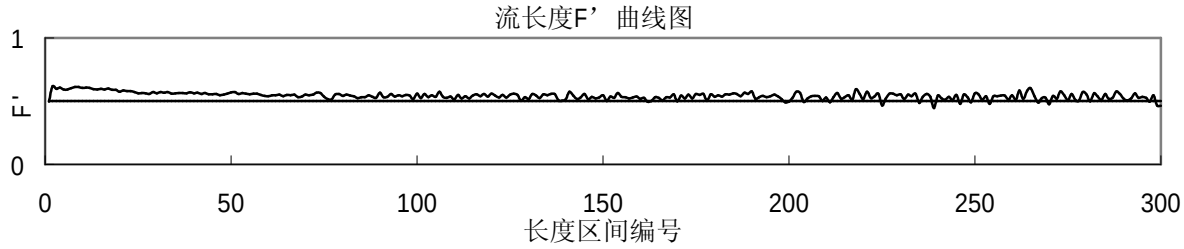

图 4 基于流字节数的加权平均非对称测度函数 F’曲线图

现得最为明显。这表明流长度的非对称属性值为 0.5—0.95 的流的数量较少。

在上述图形的基础上，根据定义 4，得到流长度的 F 函数在各分段的加权平均值—F’的曲线图如图 2 所示。

图中直线表示定义 5 中给出的非对称测度函数均值。此处为流长度均值,值为 0.500。

从图中可以看出：

（1）按照定义 5 得到均值为 0.5，这表明 TCP 流交互的双方报文数之比约为 1:3(由定义 2 公式得到)。

（2）加权后的流非对称测度与流长度没有明显关联，满足平稳性，即各流长度区间的加权流对称测度值没有明显区别。

综合以上 2 点可以看出，基于流长度的非对称测度可以作为衡量网络健康状况的一项指标，即如果在较长一段时间内数据流的非对称测度的统计值明显高于或低于 0.5，则可能发生了异常。

（3）相对而言，由于上述曲线的抖程度随流长度的增加而加剧，这表明短流的加权非对称测度更加稳定，而长流该测度的方差要大于短流，这在一定程度上与短流的数量要大大多于长流数量有关[7]。短流的非对称测度偏高的也可能与采用了比较保守的除噪声方法有关（见 2.2）。

4 流的字节数非对称性分析

本小节将所关注的流属性变为字节数，按同样的方法对上述数据进行分析。此时，由于包含字节数多的流对整体性能的影响要远远大于字节数少的流，这个因素对流字节数的影响比报文数更大，因此将取 M＝700000000，这样则在上述有效数据中，只有 99 个流的字节数超过该范围,不在统计和分析的范围内。同样取 n＝300。基于流字节数的 Fm%函

数图形如图 3 所示(为了显示清楚,将图形分为两部分显示)。

在上述图形的基础上，根据定义 3，得到流字节数的 F 函数在各分段的加权平均值—F’的曲线图。见图 4。

图中直线表示定义 5 中给出的非对称测度函数均值。此处为流字节数均值,值为 0.628。

由于 3.2 和 3.3 中的分析采用的是同样的数据源，因此将图 3 和图 4 与图 1 和图 2 进行比对，明显可以看出：

1) 流字节数的非对称测度要明显高于流长度非对称测度；
2) 流长度的非对称测度较流字节数的非对称测度更容易达到稳定，这意味这基于后者的分析需要比较大的样本容量。

5. 结论

网络行为学作为一个寻找和探索内在规律性的研究领域已经被提出很长时间了，但是相关的研究工作并没有取得预想的结果。其中研究工作缺乏有效的切入点是一个很重要的原因，缺乏一个完整的测度体系也是原因之一。另外，由于在目前的互联网环境中基于 TCP 的应用占绝大多数，面向 TCP 的流分析更有意义，因此，本文选择了 TCP 数据流的非对称性作为研究的着眼点，通过测量、统计和分析的方法得到了有关的结论:

1） 就流长度的非对称性而言，超长流的非对称性比短流和长流的非对称性明显，且超长流非对称性波动大，而短流与长流的非对称性稳定。
2） 随着流的字节数增加，数据流字节数的非对称性越发明显，波动越大。

这些结论一方面可以为网络行为学的研究工作拓展思路，另一方面，从实用角度来看，对网络负载均衡[8]和非对称链路[9]的带宽测量[10]等方面的研究也具有一定的参考价值。

本文的研究主要结论均来自于比较直观的图形分析，这是一种定性的分析，也本文的一个遗憾之处。缺乏定量分析的主要原因是由于数据量过于庞大。今后我们将基于聚类和抽样等方法研究具有更高效率的算法来进行定量的分析，并将其作用于更新的数据。另外，本文的非对称分析是忽略了方向的，这在一定程度上强化了非对称性。

最后，需要强调的一点是本文的结论是在净化后的数据上获得的，这样做的主要目的是为了能更好地体现网络的正常的行为规律。另外，在对数据的分析和处理过程中，我们还发现短流和超短流的大量存在，这是一个只有通过组流才能发现的不正常的现象，有关的研究工作正在进行，它得到的结论将更具实际意义。

参考文献:

[1] KC Claffy “Measuring the Internet” http://www.caida.org/publications/papers/2000/ieee0001/ IEEE Internet Computing Online, v4n1 January 2000

[2]B.Ryu, D.Cheney, H.W.Braun. “Internet Flow Characterization: Adaptive Timeout Strategy and Statistical Modeling”. In Workshop on Passive and Active Measurement(PAM), Apr, 2001. pp. 94-105

[3] Srinivas Shakkottai, Nevil Brownlee, K. C. Clay “A Study of Burstiness in TCP Flows” Passive & Active Measurement (PAM) workshop in 2005 page:13-26

[4] Marina Fomenkov, Ken Keys, David Moore, KC Claffy “Longitudinal study of Internet traffic in 1998-2003” Winter International Symposium on Information and Communication Technologies (WISICT) on January 5-8th, 2004 in Cancun, Mexico page: 1-6

[5]程光，丁伟，龚俭 “高速网络流量通用测量平台-WATCHER” CSIT 2004 会议论文集 南京 2004 page:122-128

[6] J. Postel. RFC 793 - Transmission Control Protocol September 1981

[7]周明中 龚 俭 “CERNET 流特性研究” CSIT 2004 会议论文集 南京 2004 page:136-140

[8] Hari Balakrishnan, Venkata N. Padmanabhan, and Randy H. Katz “The Effects of Asymmetry on TCP Performance” Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking Budapest, Hungary 1999. pp:77-89

[9] H. Balakrishnan, V. Padmanabhan, G. Fairhurst, M. Sooriyabandara, "TCP Performance Implications of Network Path Asymmetry" RFC 3449, December 2002.

[10] R. S. Prasad,_ M. Murray,_ C. Dovrolis,_ K. Claffy “Bandwidth estimation: metrics, measurement techniques, and tools” IEEE Network, November-December 2003 vol. 17, no. 6, pp. 27–35,

联系方式:
南京市东南大学华东北地区网络中心

Email:xdai@njnet.edu.cn 电话：83794000－211 邮编：210096

作者介绍：

戴宣，男，1982 年，硕士生，研究方向：网络行为学；

丁伟，女，1963 年，教授，博士生导师，博士，研究方向：网络行为学，网络安全，网络测量；

程光，男，1973 年，副教授，博士，研究方向：网络行为学，网络安全，网络测量。