CERNET 流特性研究[1]

周明中 龚 俭

（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：基于流特性的测量在网络行为分析中发挥越来越重要的作用。本文通过对一定时期 CERNET 网络流的观测，得到 CERNET 主干整体流的分布特征。在此基础上，根据长度的不同将流区分为单报文流，短流，长流和超长流，并对不同长度的流，特别是单报文流和超长流所表现的行为特性和导致这些行为特性的原因进行了进一步探讨，为路由优化和性能估计提供必要的依据。

关键词：网络流量；流特性；单报文流；超长流

Study of CERNET Flow Characteristics

Zhou Mingzhong, Gong Jian

（Department of Computer Science, Southeast Univ., Jiangsu, Nanjing 210096 China）

(Jiangsu Province Key Laboratory of Computer Networking Technology)

Abstract： The measurements based on the flow characteristics have been more and more important roles in the analysis of Network Behavior. This paper firstly analyzed and compared characteristics of different kinds of flows via observation of the CERNET backbone traffic, and concluded the whole flow distribution and behavior characteristics of this network. Based on this, single packet flow, short flow, long flow and very long flow are determined with the difference of packet number in flows. This paper analyses the behavior characteristics of different kinds of flows and the causes of them, especially the single packet flows and very long flows, which can contribute to the route optimization and capability estimation.

Key words： network traffic; flow characteristics; single packet flow; very long flow

[1] 本文受国家 973 计划课题（2003CB314803）资助

1 引言

针对流的网络行为研究在很多方面弥补了局限于数据报文层次研究的不足。所谓数据流，是指符合特定的流规范（specification）和超时（timeout）约束的一系列数据报文的集合[3]。在不引起歧义的情况下，引入 Ryu 在[3]中提出的根据包含报文的数量区分流的概念，并根据 CERNET 流分布的实际情况将流分为单报文流/短流/长流/超长流(SP/S/L/VL)：单报文流是指只包含一个数据报文的流，短流是指数据报文数量等于或小于 10 个的流，长流是指数据报文数量大于 10 且小于等于 1000 个的流，将数据报文数量大于 1000 的流定义为超长流。

2 CERNET 主干网中的流特性

由于采用不同的超时策略对流特性分析有很大的差异，本文采用不同的固定超时策略对流分布进行比较分析。在此基础上，对流分布和行为影响较大的单报文流和超长流的特性和可能的形成原因作进一步讨论。

2.1 主干的流分布

由于教育科研网相对于一般网络既存在共性又具有其特性，本文在一定时间范围内对 CERNET 主干双向流量进行观测，按照前文定义的方式组流并加以分析，得到 CERNET 主干流的特性。由于 CERNET 主干双向平均流量在 600Mbps 以上，处于高峰时超过 1.1Gbps，对如此大流量进行在线的复杂分析是基本不可行的，本文采用分时段采集和存储数据报文的方式，利用离线处理满足对相同数据源进行多次复杂分析的需求。

参考 Claffy 在[1][2]中提出的方法，用取值为 2 的幂的固定超时策略观测和比较流分布，可以得到相对准确而显著的结果。本文于 2004 年 4 月和 5 月间，采用 2 至 512 之间的固定超时方式对不同时段（AM10：00－11：00，PM20：00－21：00）的 CERNET 主干流量进行分析，获得基于报文规模和字节规模的流分布如图 1 所示。

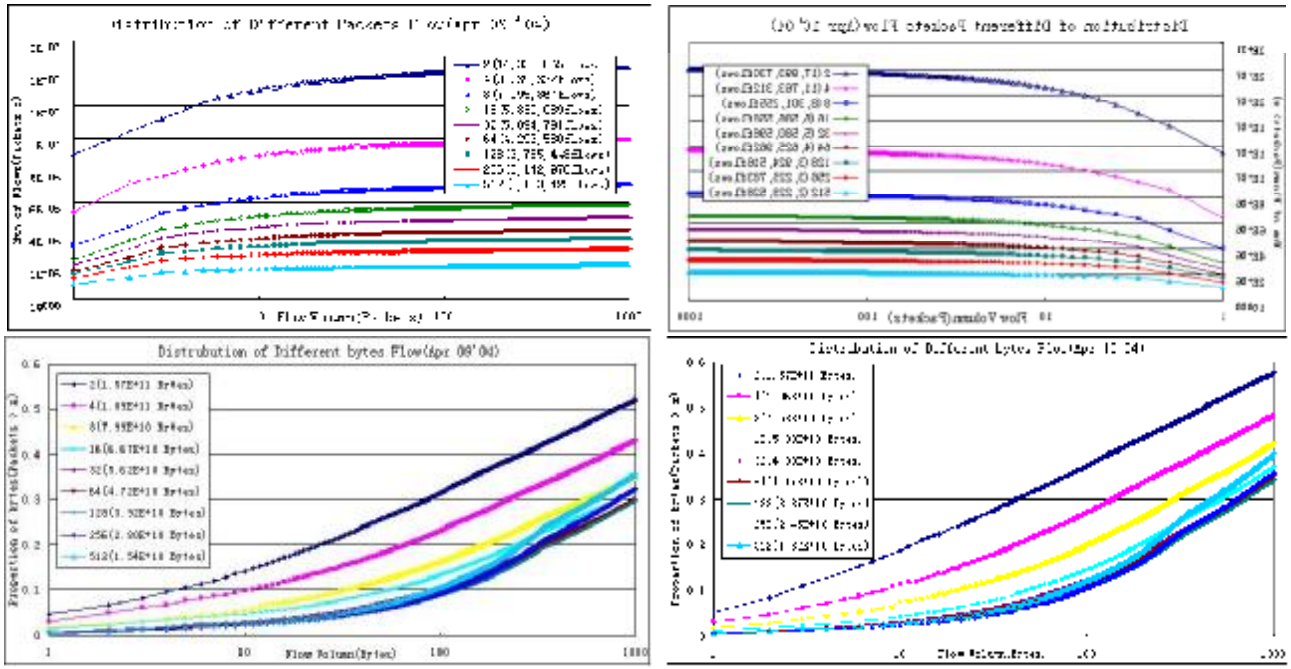

图 1 不同时间段的基于报文规模和字节规模的流分布

总体而言，在正常情况下，不同时段所反映的流分布特征是相似的。随着超时的增大，所得流的数量逐渐减小，这是因为较短的超时将较长的流截断为若干较短的流所致；而在一定时段内，较长的超时要维护更多的流，所以其所需资源也相应地增加。在超时小于 64 秒时，随着超时的增加流的数量急剧减少，而当超时大于 64 秒时，流的总量减少的速度明显减缓，在一定程度上说明了目前在流测量中普遍采用 64 秒作为默认固定超时的原因。

图 1 中基于不同时段报文数量的比较显示，不管采用何种固定超时，单报文流数占总流数比例始终维持在 40%以上；数据报文数<10 的流数（单报

文流＋短流）占流总数的 90％左右，单报文流和短流占据了流总体数量的绝对多数。 基于不同时段字节量的比较显示，长流和超长流所对应的字节数超过总字节数的 80％，而流数量只占 10%左右，特别当超时大于 64 秒时，占总流数不到 1％的超长流所占字节数为总流量的 65%以上，这表明在 CERNET 中流分布和对应数据报文的分布都呈现典型的重尾分布。

2.2 报文到达率分布

B.Rye, D.Cheney,et al.[3]详细分析了不同长流（报文数>10）的流间报文到达率的分布。在一个路径（trace）上采集前 200 个长流的报文到达时间（Packet Interarrival Times），分别其报文到来时间的协方差（cov），得到 90％的协方差小于 2，对其他不同的路径进行相同的实验结果亦相同，从而提出了属于同一个流的报文到来时间间隔是相对固定的假设。

本文在[3]的基础上，提出观测最长流的报文到达时间平均值和标准化的均方差（SMD）来表现流的报文到达率的方法。平均值表现了流间报文到达时间的分布情况，其标准化的均方差用于描述属于同一个流的数据报文在到达时间上的差异，两者的结合可以很好的分析被观测网络的拥塞情况及其他行为特征。

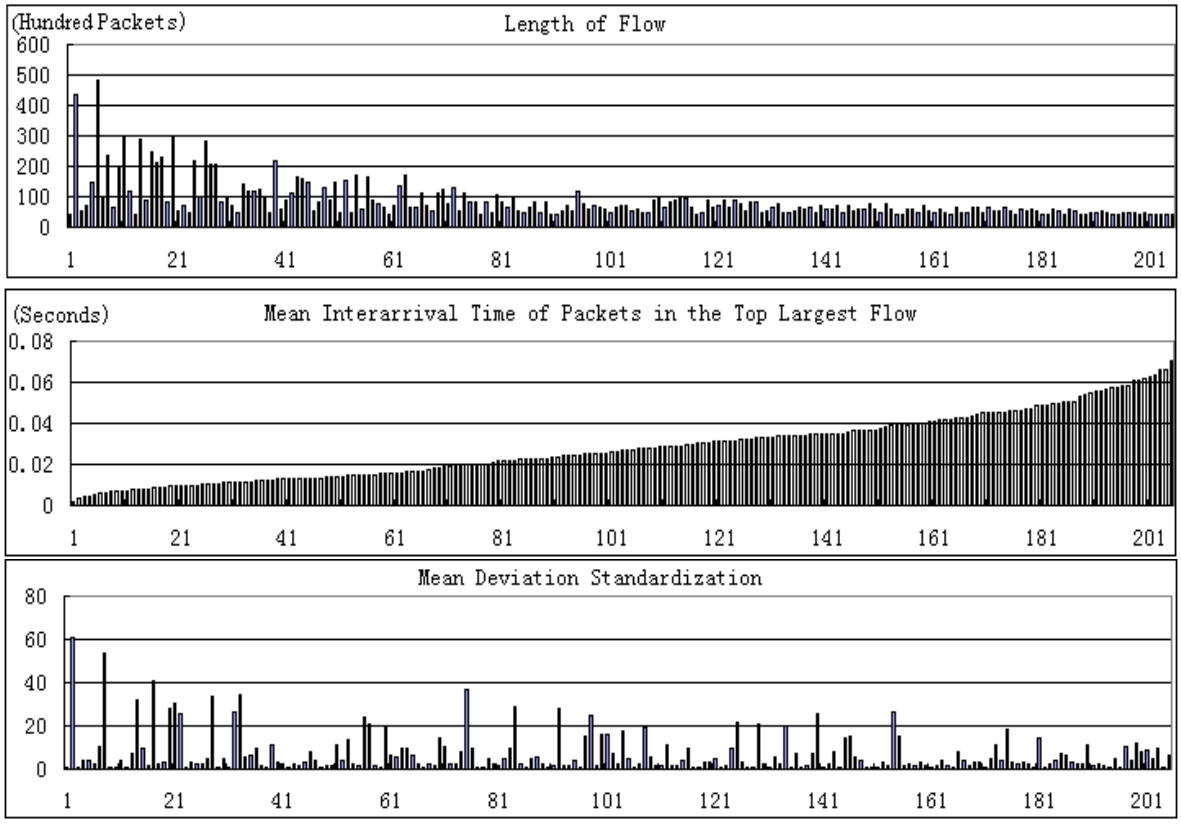

图 2 排序后的 205 个最长流平均报文到达时间及其对应标准化后的均方差

图 2 是在 CERNET 上采用固定超时策略（64 秒）观测一定时间段（2004 年 4 月 10 日 20：00－20：30），所获得的前 205 个最长流的报文到达时间的平均值及其标准化后的均方差值。其中最长的报文到达时间平均值为 0.070597 秒，平均值为 0.028166 秒，均远小于 1 秒，该值与流的长度不存在对应的关系，这说明在正常情况下，CERNET 上长流具有较高的报文到达率，且报文到达率与流的长度无关。标准化均方差值 SMD 是采用均方差值除以平均值获得的，该值越大则表示报文到达时间最大值和最小值之间的差异越大，从图 2 观测和计算的结果来看，SMD 平均值为 7.253019，且有 70%以上的 SMD 小于平均值，从而论证了 Rye 提出的观点：流间报文达到时间趋向于一种持续状态。

对其他时间段的测量和计算结果与上述实验结果相类似，报文到达时间均值在 0.03 左右，SMD 平均值都在 10 以下，且其中 70％以上均小于平均值。

2.3 报文长度分析

不同长度的流中报文长度的分布也是各不相同的。从长时间统计数据来看，一般而言，流中包含报文的平均长度随着流长的增加而增加。表 1 是针对　　年 月 日一个小时内（20：00－21：00）所有流报文长度统计的结果，数据显示除比较特殊的单报文流之外，流的平均报文分布是符合以上提出的统计结论的。其中占流总数只有 0.1%左右的超长流报文平均长度为 666 字节，由于在实验中还发现大部分超长流两个方向的报文数量大致相当，但报文长度是不对称的，也就是说超长流的有效载荷大部分集中在一个方向上，由此可以推断超长流一般由于提供文件传输，流媒体等大数据量的服务而产生的，这些服务有数据量很大，数据交互的不对称等特点。长流的报长相对较短，而且有效载荷的不对称性不是十分明显，但其数据报文数占总数的一般以上（57.4%），其中一个端口为 80 流占据了其中的较大比例。可以推测，一般的 Web 访问服务是其产生的主要原因之一，其他如 Email 等服务也在其中占一定比例。短流的数量相对较多（37.5%），但由于流长度较短，所以其报文数量只占报文总量的 7.8%，主要是由 Web 服务所产生的。

表 1 不同流的报文平均长度和数量比较表

种类	平均报文长（pkt/flow）	流数量（比例）	报文数量（比例）
单报文流	488	4125133（50.1%）	4125133（2.8%）
短流	118	3086107（37.5%）	11287298 (7.8%)
长流	206	1009429（12.3%）	83556254 (57.4%)
超长流	666	7824（0.1%）	46586895 (32.0%)

单报文流由于只包含一个报文，所以其只占总报文数量的 2.8%，但其数量是流总量的 50.1%。其长度分布相对比较分明：长度小于 100 字节的短报文占其中大多数，比例约为 62.9%；而由于也包含相当数量的长度大于 1200 字节的长报文（约占 26.2%），所以导致单报文流平均报文长度较大，表 1 所示其值为 488 字节。

3 流特性分析

3.1 单报文流特性分析

图 1 的实验结果显示在 CERNET 网络中存在大量单报文流，分析这些单报文流的构成，可以从很多程度上揭示网络中流分布的特性，为进一步的网络行为研究提供依据。考察传输层协议（TCP，UDP）可知，两个主机之间正常的通讯至少需要两至三次交互，所以绝大多数单报文流应属于主机之间的非正常交互。

本文在 CERNET 流检测过程中随机地抽取 10000 个单报文流并根据其源宿端口进行排序，得到使用最频繁的 7 个端口比较表如表 2 所示。

表 2 单报文流使用最频繁的端口比较表

应用层协议	端口号	总数	宿端口数
HTTP	80	2113	1793
Location Service	135	1198	1198
Microsoft-DS	445	1187	1186
FTP	21	379	319
DNS	53	346	252
NETBIOS NS	137	220	220
NETBIOS SS	139	52	51

由表 2 可知使用这些端口的单报文流占其总量的 50%以上，其他单报文流所使用的源宿端口一般均为高端端口。表 1 提供的数据还表明公认端口绝大部分甚至全部为单报文流的宿端口，如 135 端口，445 端口，137 端口，139 端口等，可以推断这些单报文流都是由源主机发起的对目的主机相关公认端口的探测，且没有大部分没有的到回应（否则可以观测到目的主机相关端口对源主机的响应）。

从所属类型上看，包含 80 端口的单报文流占总数的 20%以上，分析其主要原因是 80 端口是目前网络中提供服务的主要端口，除了常用的 Web 服务，还有很多网络应用特别是代理（proxy）服务也是通过它所支持的，所以成为网络探测的主要对象；提供其他服务的端口如 135 端口和 445 端口，在通用的操作系统（Windows 系列和部分提供 SMB 服务的 Linux 系统）中是默认打开的，也成为网络

探测的主要关注对象。

3.2 超长流特性分析

从多次随机抽样的结果来看，超长流都是由 TCP 和 UDP 构成，其他流的形式（ICMP 等）是几乎不存在的，其中 TCP 流又占超长流中的多数。超长流一般使用的端口号均超过 1024，为非公认端口，所以不能单纯通过超长流的端口号来判断流在应用层所提供的服务内容。作者通过观测位于这些超长流前后对应源宿主机之间的交互和使用的端口号来推测可能提供的服务内容，这主要是基于目前 TCP/IP 协议簇相关应用协议的特点做出的判断，如在网络中存在的 FTP 协议一般采用被动方式，客户机通过 21 端口和服务器建立联系后会使用协商机制采用一对高端端口进行实际文件的传输。

表 3 超长流使用最常的端口比较表

IP 层协议	端口及相邻报文端口	数量	比例
TCP	80	1338	39.72%
TCP	21	647	19.24%
TCP	8080，1080，8000	67	1.99%
UDP	53	14	0.42%

本文观测了 2004 年 4 月 25 日（00：00－23：00）12 个不同时段采集数据，对随机选出的 3369 个超长流及其前后各 3 分钟之内流的交互进行分析，获得最常使用端口比较如表 3 所示。

抽样数据显示这些超长流均由 TCP，UDP 构成，其中 TCP 占总数的 89.55%，而其中大部分 TCP 流使用 80 端口和 21 端口（分别占 39.72%和 19.24%），也就是说明了超长流主要是由 Web 服务和 Ftp 服务产生的（个别主机可能使用 80 端口作为提供代理服务的端口）。测试数据还表明使用 8080，1080，8000 端口交互的超长流占有一定比例，这些端口是目前普遍使用的代理软件（如 squid 等）的默认端口，在 CERNET 中有一定流量是代理服务器产生的，而且存在一定数量的代理服务器并不使用默认端口提供服务，所以实际使用代理服务产生的流量要高于实测所得的数据。在 UDP 服务中，使用 53 端口的 DNS 服务产生的超长流占一定比例，一般来说 DNS 服务是不需要产生超长流的，所以可以推测这些超长流可能是由于 DNS 配置错误或者非正常使用（如黑客攻击等）所产生的。

4 结论和未来展望

目前，对网络流量的研究已经由单纯的数据报文特性研究转向报文和流特性研究同步进行，相互补充。

本文通过对 CERNET 主干网一定时期内流的分布进行了详细的比较分析，对其流特性进行了详细的分析，并对流特性的形成原因进行了合理推测。为路由优化，区分服务和网络性能优化等基于流的网络性能提高提供了必要的技术支撑。

本文只对目前 CERNET 主干网中流的分布和部分特性进行了较详细的阐述，并没有对一定时期流到达和离开率做详细的分析；由于对产生流的应用背景进行了初步的推测和判断，但没有进一步对流及其与其相关的高层协议作具体的分析和对照，所以并不能评估推测的准确性。这些都是未来研究的重点。

参考文献

[1]K.C.Claffy. Internet traffic characterization. Dissertation for the degree Doctor of Philosophy. University of California, San Diego.1994.

[2]K.C.Claffy, H.W.Braun, G.C.Polyzos. A Parameterizable Methodology for Internet Traffic Flow Profiling. In IEEE Journal on Selected Areas In Communications, Vol.12, No.8,Oct. 1995.pages: 1481-1494.

[3]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.

[4]R.Jain and S.A.Routhier. Packet trains-measurements and a new model for computer network traffic. *IEEE JSAC*, 4:986-995, 1986.

[5]A.Shaikh, J.Rexford, K.G.Shin. Load-Sensitive Routing of Long-lived IP Flows. In *Proceedings of SIGCOMM*, September 1999.

[6]N.Hohn, D.Veitch. Inverting Sampled Traffic. In *IMC'03*. Oct.2003. Miami Beach, Florida, USA.

[7]G.Iannaccone, C.Diot,et al. Monitoring very high speed links. In *IMW'01*. Nov, 2001. San Francisco, CA, USA.

[8]N.Duffield, C.Lund, M.Thorup. Properties and Prediction of Flow Statistics from Sampled Packet Streams. In *IMW'02*. Nov, 2002. Marseille, France.

[9]S.Dharmapurika, P.Krishnamurhty, D.E.Taylor. Longest Prefix Matching using Bloom Filters. In *SIGCOMM, 2003*. Sept, 2003.

第一作者信息：
姓名： 周明中
单位： 东南大学计算机系华东北地区网络中心
地址： 南京市四牌楼 2 号
邮编： 210096
电话： 025－3794000－206
Email： mzzhou@njnet.edu.cn
简单介绍：周明中，男，博士生，主要研究方向：网络行为学。