第 34 卷 第 6 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.6 Computer Engineering March 2008
·网络与通信· 文章编号：1000—3428(2008)06—0112—03 文献标识码：A 中图分类号：TP393.02

大规模网络中 IP 流长分布统计模型

吴 桦，周明中，龚 俭
(东南大学计算机科学与工程学院江苏省计算机网络技术重点实验室，南京 210096)

摘 要：对具有不同特征的大规模高速网络的 TRACE 进行分析，发现不同 IP 流的流长分布特征。在此基础上，提出大规模网络状况下 IP 流长分布经验模型，该模型在表达大规模网络 IP 流长分布上，其精度高于原有 Pareto 模型，复杂度低于原有双 Pareto 模型。对相关模型与实际 TRACE 流长分布的拟合程度进行了检验，并对模型的相关参数取值范围及该经验模型与现有模型存在的异同做了讨论，进而分析导致异同的原因，并指出 IP 流长分布的发展趋势。

关键词：网络被动测量；网络行为；大规模网络；IP 流长；分布统计模型

IP Flows Length Statistical Distribution Model in Large-scale Networks

WU Hua, ZHOU Ming-zhong, GONG Jian
(School of Computer Science and Engineering, Jiangsu Province Key Lab of Computer Networking Technology, Southeast Univ., Nanjing 210096)

【Abstract】 This paper studies TRACEs with different characteristics. The flows length distribution characteristics are discovered by analyzing those TRACEs. Based on the discussions, the empirical model of IP flows distribution for large-scale networks is proposed based on the characteristics analysis, whose precision is better than Pareto model, and the complexity is less than double Pareto model. Goodness-of-fit test is employed to inspect the effect of this model and its parameters. And then, this empirical model is contrasted with other distribution models presented by former researchers, and the same and different characteristics among all of these models are discussed, and so do their causes. The possible tendency of IP flow distribution is forecasted based on those discussions.

【Key words】 network passive measurement; network behavior; large-scale networks; IP flows length; statistical distribution model

1 概述

IP 流是符合特定的 IP 流规范约束的一系列数据报文的集合，IP 流长分布直观地反映了各种类型和长度的 IP 流对网络总体流量的贡献，它不但可以反映由 IP 层协议导致的网络相关特性，也可以反映网络使用者的使用偏好以及这些偏好对网络运行的影响。

文献[1-4]的结论表明，研究网络中传输文件的大小及其分布可以为路由策略、流量建模和网络安全等相关应用提供决策依据。实际环境中 IP 流不仅包含表现为文件大小的实际负载，还包含网络中用于传递控制信息的流量，以及由恶意网络行为或配置错误所导致的其他背景流量，这些流量报文的存在会对 IP 流的流长实际分布产生影响，因此基于传输文件大小的网络负载预测和表述并不能完备地表述网络的实际负载情况。文献[5]虽然详细地测量和分析了大部分 IP 流(包括 TCP 流和 UDP 流)流长在网络中的分布情况，但是该文献的研究存在以下 3 处不足：(1)忽略了 ICMP 流对流总体的影响。 (2)该文献所选取的研究对象为来自于一个局域网多个时段的流量，不能从普遍意义上描述 IP 流在大规模网络中的实际分布状况，如 ICMP 报文的比例就比较低。(3)该文献在研究过程中并没有对 IP 流的所有构成成分进行分析，将其中存在的异常 IP 流也纳入 IP 流长分布的观测模型中，因此在描述 IP 流长分布时可能会出现较大的偏差，而这种情况在描述不同网络的 IP 流长分布时可能表现更为严重。针对上述问题，本文使用从互联网主干网采集的观测数据，对大规模网络中 IP 流的流长分布进行了系统性的研究和探讨。

2 IP 流长总体分布特征

2.1 数据来源

本文所选取的 TRACE 主要来自于：(1)CERNET 华东北地区网络中心；(2)美国互联网研究国家实验室(NLANR)公开提供的 TRACE。CERNET 系列 TRACE 的采集点位于江苏省教育网边界路由到国家主干路由之间；其他 TRACE 均来自于美国互联网研究国家实验室在不同时间对不同网络采集的结果。本文选取了从 2001 年~2004 年，不同采集点、不同带宽的 8 个 TRACE 作为分析对象。

2.2 不同 TRACE 的 IP 流长实际分布

由于对大多数网络而言，主要存在的 IP 流根据不同的协议类型可以大致分为 3 类：TCP 流，UDP 流和 ICMP 流。这 3 类 IP 流在绝大多数网络中承载了 99.9%以上的流量，所以本文主要研究不同状况下，3 类协议类型的 IP 流在不同负载状况下的流长分布状况。

图 1 描述了来自 3 个不同 TRACE 的 4 类 IP 流的流长分布曲线，IP 流采用五元组的方式定义，并使用 64 s 的固定超时标识流的终结。为更加清晰地表达流长的分布状况，相关数据均使用双对数曲线表示。

基金项目：国家“973”计划基金资助项目(2003CB314803)；国家“863”计划基金资助项目(2005120AA103011-1)；教育部科学技术重点研究项目(105084)

作者简介：吴 桦(1973－)，女，博士研究生，主研方向：网络行为学；周明中，博士研究生；龚 俭，教授、博士生导师

收稿日期：2007-03-22 **E-mail：**hwu@njnet.edu.cn

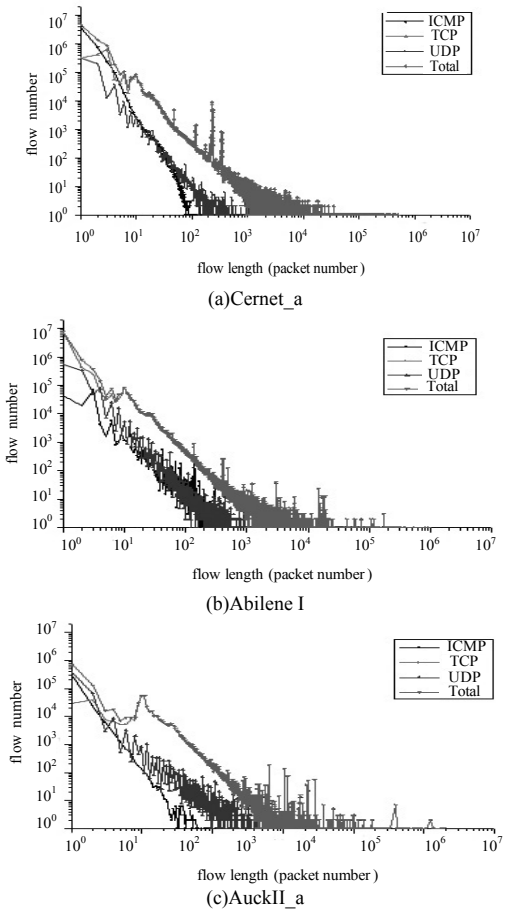

图 1　不同 TRACE 的不同类型 IP 流长分布曲线

从统计结果来看，在不同网络不同负载的情况下，IP 流长的总体分布呈现明显的重尾分布特征：IP 流长分布的范围比较广，但是流长小于 10 的 IP 流占 IP 流总量的 90%以上(为方便描述，本文将流长小于 10 个报文的 IP 流称之为短 IP 流)。这一点和文献[5]的研究结果相吻合。

从总体上看，TCP 流长分布在绝大部分情况下和 IP 流长分布几乎是重合的，所以 TCP 流长的分布特征主要反映了 IP 流长的总体分布特征；但统计数据表明，在所有 TRACE 中，ICMP 流和 UDP 流都占有相当的比重，这 2 种类型 IP 流对总体分布的影响主要位于流长较小处(短 IP 流)。因此 TCP 流在一般情况下，流长要大于 ICMP 流和 UDP 流。

下面分别针对 TCP 流、UDP 流、ICMP 流分析其流长分布情况。

TCP 流长分布从总体上看服从重尾分布的特征，随着流长的增加，TCP 流的数量呈指数减小的趋势；但是来自不同 TRACE 的实测数据同时也表明 TCP 流并不是严格服从均一的重尾分布，均存在一定数量的与分布特征相违背的地方。如在所有 TRACE 中，流长为 10 左右不同程度地存在这样的流数量突然增加的现象，对其他 TRACE 分析结果表明这一现象也明显存在；在 CERNET 中，在流长为 62, 126 和 254 左右均存在流数量突然增加的现象；具体的分析表明这些异常均是由网络恶意行为或配置错误造成的。

UDP 流长分布也基本服从重尾分布的特征，但是因为其所承载的流量相对于 TCP 流而言要小得多，所以其尾重相对于 TCP 流较小，而且并没有像 TCP 流一样存在明显的流数量突变情况。但是不同的 TRACE 中，UDP 流长分布曲线都呈现明显的锯齿状，流长为奇数的 UDP 流在数量上明显小于流长为偶数的 UDP 流。由于本文定义的 IP 流为双向流，可以推测，绝大部分 UDP 流双向报文具有明显的对称性。

从不同 TRACE 的观测结果来看，ICMP 流的最大流长基本都在 100 左右，也就是说，如果假设 ICMP 流双向报文数量为 1:1，ICMP 流最多完成 50 多次交互。而即使 ICMP 流的最大流长维持一个较小值，ICMP 流的流长分布也依然服从重尾分布的特征，流长较小的流占总体流数量的绝大多数，流长为 1 的 ICMP 流在所分析的 3 个 TRACE 中所占比例均大于 50%。

对其他 TRACE 的分析也获得了类似的结果，由于篇幅所限，这里不一一列出。

3　IP 流分布的统计模型

前期的研究发现，在网络中传递的大部分文件(数量在60%以上)平均长度都小于 10 KB，Web文件的长度分布基本服从Lognormal分布[1-2]。文献[4]基于Downey A的研究提出了文件大小分布呈双Pareto和三Pareto分布的模型。这些研究试图从Web文件的长度分布推测网络中TCP流的长度分布，这对于以Web流量为主的网络无疑是基本正确的，但是随着网络的发展，网络应用的主要构成部分已经发生了改变，原有模型可能已经不再适用。网络流量的实际组成部分不仅由用于传输文件的报文构成，还包括相当数量的用于传输流媒体(如UDP类型的RealMedia)和用于控制的报文(如用于探测主机可用性的ICMP报文)，IP流(包含TCP流、UDP和ICMP流)的流长分布可能与前期基于Web流量的建模存在相当的差异，而也只有从IP流的角度才能真实反映网络的实际负载，因此有必要对IP流长分布进行测量统计和建模。

众多文献研究表明[1-3,5]，无论是用五元组的方式、源宿地址还是宿地址宿端口的流规范，Internet中IP流长均服从重尾分布，本文在第 2 节使用五元组流规范对所有TRACE中IP流长分布的研究也证明了这一点。但是IP流长分布到底服从哪种类型的重尾分布，在不同规模的网络中，IP流长分布是否存在可以同一类型的重尾分布模型？本节在探讨常用重尾分布模型异同的基础上，逐一解答以上问题。

3.1　重尾分布模型描述

所谓重尾分布是指集合中相异元素大部分出现的次数很小，但有一小部分元素出现的次数(频率)十分高，以至于它们的数量和占集合中的绝大部分。重尾分布模型尾部减小不是按照线性方式减小的，而是按照近似双曲函数曲线的方式减小，因此一般重尾分布函数曲线的渐近线是一条单边双曲函数曲线。重尾分布的表达模型有多种，常用的分布模型主要有 Pareto 模型，Lognormal 模型和 Weibull 模型等。3 种不同重尾分布函数的补累积分布曲线(CCDF)比较如图 2 所示。

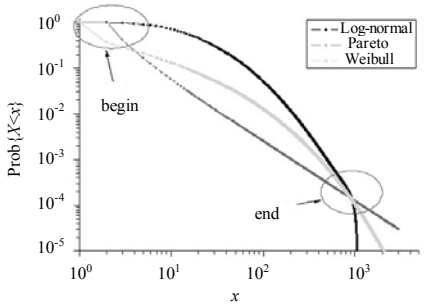

图 2　尾重近似的不同重尾分布函数的补累积分布曲线比较

在图 2 中，3 种不同重尾分布函数的补累积分布曲线(CCDF)比较如图 2 所示，坐标采用 Log-Log 的模式，其中

Pareto 函数的参数 α=1.3, k=2 ;Weibull 函数的参数为 α=0.32, λ=1；Lognormal 函数的参数为 μ=2.8, σ=1.1。从三者的累积分布曲线可以看出，同样是表达重尾分布特征，三者在分布上具有明显的区别。Pareto 函数分布曲线在 Log-Log 情况下为一条直线，该直线的斜率为-α，所以该函数随着 x 的增加呈指数衰减；而 Weibull 函数的分布曲线随着 x 的增加呈稍弱于指数衰减，而其在初始阶段的衰减速度要高于 Pareto 函数；Lognormal 函数的分布曲线随着 x 的增加，其衰减速度在起始阶段要远低于前两者，但是其表达的重尾特征相比前两者有所减弱。

3.2 大规模网络中 IP 流长分布统计模型

从实际测量结果看，网络中 IP 流长分布的重尾现象相对于文件长度分布而言更加明显，这主要是因为网络中存在由冗余报文形成的 IP 流，这些 IP 流的数量较大但是流长都非常短，它们的存在严重影响了 IP 流的分布，而且由于主干网络中背景噪声各不相同，在分析 IP 流分布时需要除去这些由冗余报文所产生的 IP 流，才能反映网络中由于正常交互 IP 流的流长分布特征。本文在将各 TRACE 中由冗余报文导致的 IP 流剔除之后，将所有 TRACE 的 IP 流长分布的 CCDF 曲线用图 3 描述。

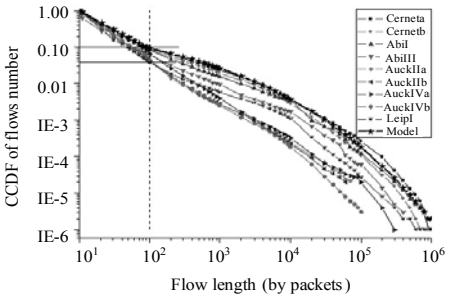

图 3 冗余消除后 IP 流长分布

从对 TRACE 数据的实际分析中可以发现，流长大约为 10 处， Web 应用导致了 IP 流数量发生突变，但这种突变并不是由冗余报文所导致的，因此在考察 IP 流分布时，应当将其划入考察的范围。从所有 TRACE 分析的结果看，IP 流长在 10~100 之间的 CCDF 曲线在双坐标系内基本可以用斜线拟合；而流长大于 100 之后，CCDF 曲线下降趋势减缓，可以用 Weibull 分布拟合。图 3 采用曲线的拟合方式获取流长大于 10 的 IP 流的分布模型，从拟合结果看，模型的曲线和高速 IP 流的流长分布曲线基本吻合。

$$P(X \ge x) = \begin{cases} 1 - kx & 1 \le x < x_0 \\ k \cdot (\frac{c}{x})^{\alpha} & x_0 \le x < x_1 \\ k \cdot \exp\{-(\lambda x)^{\beta}\} & x > x_1 \end{cases} \quad (1)$$

根据IP流的分布特征，本文假设x_0和 x_1分别取值为 10 和 100，针对从大规模高速网络中获得的TRACE中IP流长分布进行分析，采用数据拟合的方式，估计式的各个参数分别如下：k = 0.06, c=10.0, α=1.06, λ=1.0, β=0.19。

从参数分析可以看出，在不考虑无应答 IP 流的情况下，IP 流长的分布基本可以使用 3 个不同的曲线进行拟合。

3.3 Kolmogorov-Smirnov 拟合优度检验

Kolmogorov-Smirnov(K-S)拟合优度检验是一种基于经验的分布函数(ECDF)检验方法，用于检验待测连续分布 $F(x)$是否服从一个已知分布函数 $P(x)$。

Kolmogorov定理：假设已知一个连续分布函数$F(x)$，样本(x_1, x_2, …, x_N)取值自分布$F(x)$，$S_n(x)$为$P(x)$所对应的经验分布函数，记

$$D_n = \max_{-\infty<x<+\infty} |S_n(x) - F(x)|$$

则

$$\lim_{n\to\infty} P\{\sqrt{n} D_n \le \lambda\} = L(\lambda) \qquad (\lambda > 0)$$

其中，$\lambda = 1 - 2\sum_{j=1}^{\infty} (-1)^{j-1} \exp\{-2j^2\lambda^2\}$。

由此假设H_0：$S_n(x)$=$F(x)$为真，则当 $n \to \infty$ 时，$\sqrt{n}D$ 的分布函数将收敛到$L(x)$，因此设D的观测值为d，则当

$$\alpha = P\{\sqrt{n}D > \sqrt{n}d\} = 1 - L(\sqrt{n}d)$$

为一个较小的值时，拒绝该假设。

在实际计算中，针对不同的样本数和置信度，有对应K-S表可供查询判断假设是否成立。95%的置信区间内，当样本数大于 35 时，如果D的取值小于 $1.36/\sqrt{n}$ ，则认为假设H_0成立。

分别对本文所研究的TRACE使用K-S检验，结果如 表 1 所示。通过查询K-S表并作相关运算可得，如果假设在 95% 的置信区间内成立，则对于各分布函数：对分布函数f_1，$D_{\max}$ 的取值为 0.432 ；对分布函数 f_2 ， $D_{\max}$ 的取值为 $1.36/\sqrt{n} = 1.36/\sqrt{90} = 0.143$ ；对分布函数f_3， $D_{\max}$的取值为 $1.36/\sqrt{n} = 1.36/\sqrt{336} = 0.074$。因此通过对流分布函数分段检验的结果显示，在 95%的置信区间内CERNET系列和Abilene系列中除AbileneIII的d_2值偏高之外，其他均满足H_0假设成立。通过对实际数据的分析可知，AbileneIII在IP流长为 10 附近出现大量的目的端口为 1433 的TCP流的链接试探，怀疑为大规模人为攻击或者蠕虫攻击导致了这部分IP流数量异常，也直接导致了所测得的数据在这段区间内不能通过K-S检验。若忽略这一段IP流数量异常，重新计算可得d_2= 0.076，满足H_0假设。

表 1 分布函数拟合的 K-S 参数检验

TRACE	f_1		f_2		f_3	
	d_1	n_1	d_2	n_2	d_3	N_3
Cerneta	0.182	9	0.096	90	0.011	336
Cernetb	0.202	9	0.015	90	0.010	336
AbileneI	0.394	9	0.096	90	0.019	336
AbileneIII	0.242	9	0.287	90	0.033	336
AucklandII_a	0.327	9	0.138	90	0.054	336
AucklandII_b	0.334	9	0.174	90	0.052	336
AucklandIVa	0.354	9	0.096	90	0.039	336
AucklandIVb	0.362	9	0.175	90	0.052	336
Leipzig-I	0.273	9	0.170	90	0.053	336

Auckland系列和Leipzig-I等TRACE，对分布函数f_2，大部分均未能通过检验，对分布函数f_3，虽然通过了检验，但是由于尾重较大，长IP流所占比例随着流长的增加呈指数级减小，因此即使能够通过K-S检验，并不能表明这些TRACE与模型不存在较大的差别。

4 与现有分布模型比较分析

从图 3 中 Auckland 系列 TRACE 中 IP 流长 CCDF 的分析可以看出，这些 IP 流所表现出的尾部特征基本可以使用 Pareto 模型和/或 Lognormal 模型来描述，这主要因为在 Auckland 系列 TRACE 中，Web 流量占绝对的地位，而且 TRACE 的采集点位于校园网的边界，因此流量的组成成分相对单纯，主要表现为 Web 流量的特征。

随着新应用的出现，在很多网络中 P2P 流量取代 Web 流量成为网络中最主要的流量。笔者所在课题组对 CERNET 主

(下转第 117 页)