第16卷 第7期
2006年7月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.7
Jul. 2006

网络测量及其关键技术

潘 飞，高 岭
（西北大学，陕西 西安 710069）

摘 要：讨论网络流量测量的常用方法和常用测量指标以及网络流量测量中的关键技术。介绍了时延测量、“噪声”分组过滤、丢包率测量、时钟偏移影响的消除等几种网络测量中常用的关键技术。通过对这些关键技术的分析，探讨了各种测量模型以及存在的问题。由于网络快速发展，新应用不断提出，网络正变得越来越复杂。为了应付日益复杂的网络，必须提出新型的网络测量方案，为整个网络稳健、可靠、高效的运行提出重要依据。

关键词：网络测量；主动测量；被动测量
中图分类号：TP393.06　　**文献标识码**：A　　**文章编号**：1673－629X(2006)07－0099－03

Network Measurement and Its Key Technologies

PAN Fei, GAO Ling
(Northwest University, Xi'an 710069, China)

Abstract: Discuss the common methods, measurement parameters and key technologies in network measurement. Several common key technologies in network measurement, such as delay, packet losing, filtering out of "packet noise" and removal of clock skew, are iotroduced. Some measuring models and issues are discussed through the analysis of delay, packet losing, filtering out of "packet noise" and removal of clock skew. Because of the fast development of network and the continually advance of new applications, network is becoming more and more complex. In order to deal with the complex network, it is necessary to put forward new measurement models, which is important basis for moderate, reliably, effectively operating of network.

Key words: network measurement; active measurement; passive measurement

0 引 言

随着网络规模的高速发展，以及语音和视频等实时业务和多媒体应用的普及，互联网的控制机制和行为特征越来越复杂和难以理解。最近对互联网网络流量的研究表明，数据包的到达不服从泊松分布，并且具有突发性，其突发程度远远超出根据泊松过程分析得到的结果[1]。这样，诸如排队论等以前的经典网络分析方法，已不能有效地对网络状况进行分析。因此，为了更深入地认识、了解互联网，提高网络服务质量，对网络结构进行更好的规划，都需要对网络流量进行测量，以解决诸如用户需要短的传输等待时间，电子商务应用需要良好的信息安全保障能力，科研人员需要验证新算法、新协议的有效性等随着互联网发展所暴露出一些问题。

1 网络测量的方法和常用指标

网络测量是要对网络的状态进行测量。但是，网络状态并没有具体的定义。事实上，网络状态是一个很抽象的变化量。由于网络终端以及网络的中间节点不可能相互了解各自的准确性能以及当前的状态，所以网络的状态是一个隐藏的变量。网络终端要想知道网络的当前状态，只有通过衡量发送和接收数据流的效果来进行评估。这些数据流可以被认为是测量它们所经路径状态的检测数据包，但是通过它们所得到的信息是不完全的并且误差也很大。因此，采用测量数据包进行网络测量是很必要的。

网络测量可分为主动测量和被动测量两种方式。主动测量是通过主动产生流量直接测量网络的属性，但是会对被测网络流量的性能产生负面的影响，因此，主动测量系统开发需要仔细考虑对网络实际传输流量的影响；被动测量完全取决于被测网络中目前已有的流量，它的最大优点是在测量期间不影响被测网络的流量，但会引起测量、分析、存储等资源短缺的问题。

1.1 主动测量技术

主动测量可以引起网络部件的特殊响应（如：traceroute），也可以用于观测网络的性能（如：treno）。主动测量给网络增加潜在的荷载负担，特别是如果没有仔细设计使得该方法产生的流量最小，那么附加的流量会扰乱网络，影响分析结果。例如：如果为了测量在IP网络中瓶颈链路的带宽，定期地向网络发送巨大的TCP传输，由此产生的附加流量可能会引起Heisenberg效应，并使测量的网

收稿日期：2005－10－31
作者简介：潘 飞（1974－），女，黑龙江大庆人，硕士研究生，研究方向为网络测量与服务质量；高 岭，教授，研究方向为计算机网络性能分析、服务质量及其应用研究。

络吞吐量低于实际瓶颈链路的带宽。其次,主动测量至少要多个网络部件以某种形式的参与,如:使用 ping 估计主机 A 到主机 B 的 RTT,需要主机 B 响应 ICMP ECHO 请求信息。

网络拓扑结构的变化需要使用主动测量技术,CAIDA 开发的 skitter 动态测量工具可用于动态发现和绘制全球 Internet 拓扑。另外主动测量技术可以探测网络的具体问题,如发现许多 Internet 端至端的延迟分布具有重尾特征。

1.2 被动测量技术

被动测量需要在网络中的一点收集流量信息,如使用路由器或交换机收集数据或者使用一个独立的设备被动地监测通过被测量网络链路的流量。被动测量的优点是可以完全取消附加流量和 Heisenberg 效应,但有些被动测量相当困难:如决定分组所采用的路由。当然如果用户关心的不是完整的网络路由,而是 AS(Autonomous System)之间的路由,那么可以被动监测两个对等 BGP(Border Gateway Protocol)之间的流量,因为流量包含全部的 AS 之间的路由信息。被动技术的另一个重要的问题是现在正在提出的要求确保隐私和安全的矛盾。

被动测量还有许多其它的应用,如:识别、刻划和跟踪网页缓冲和代理的优化配置;网络体系结构的安全性;拥塞控制算法的有效性;流量增长是由于用户数量的增加还是每个用户流量的增加;流行协议和应用使用的变化;新的技术和协议(如:组播和 IPv6)的渗透力和影响等等。这些被动测量的应用是 Internet 流量行为研究的重要内容。

有时为了能够从被动收集的数据中提取某些参数可能需要借助于主动测量。

1.3 网络测量指标

在一个运行的网络中,人们希望定义一系列的定量参数用以描述网元、链路、端到端的路径以及路径和网络设备集合(Clouds)性能和可靠性,使得用户和网络运营商对网络性能和可靠性具有最精确全面的理解。将这些经过严格定义的定量参数称为测量指标。

目前 IPPM 工作组(IP Performance Metrics Working Group)[2]定义的指标如下:

1) 连通性(Connectivity)[3]。

连通性指在某时刻 T,源地址发送某种类型的包可以到达目标地址。主要用于描述网络的可靠性,是网络业务完成的基本条件。

2) 单向延迟(One-way Delay)。

假设数据报的源地址 Src 和目标地址 Dst,在 T 时刻从源地址 Src 发送数据包 P,在 $T+\triangle T$ 时刻目标地址 Dst 收到该数据包的最后一个 bit,则单向延迟为 $\triangle T$。延迟直接影响应用的性能,造成传输层协议流控机制实施极其困难。延迟一般由三部分组成:传输延迟,传播时延以及排队等待时间。测量单向延迟的意义在于:Internet 中路径往往是非对称的(Asymmetric Paths)[4],或者即使路由是对称的但双向具有不同的性能特征,或者有些应用的性能只依赖于单向延迟(使用 TCP 进行文件传输)。

3)单向丢包(One-way Packet Loss)[5]。

网络发生拥塞使得路由器缓存溢出或数据包延迟过大而数据包丢失。丢包进一步造成数据包在网络中重传,网络负载增大,性能恶化。单向丢包根据一次测量数据包发送数量的不同可以分为单次测量单向丢包(Type-P-One-way-Packet-Loss)和多次采样测量丢包。

4)双向延迟(Round-trip Delay)[6]。

网络应用往往需要客户机和服务器之间发送请求和应答,以完成信息传递。网络中路由不对称性的存在,使得只有测量双向延迟才能得到完成一次握手不同路径的总延迟。相应地,双向延迟也可以分为单次测量双向延迟(Type-P-Round-trip-Delay)和多次采样测量双向延迟。

2 网络测量中的几个关键技术

2.1 时延测量

时延测量首先要消除测量中出现的随机性。如同任何测量一样,对网络的时延测量存在很大的随机性。其次是对单向时延的测量,必须保证网络入口点和出口点的时钟同步。如果时钟不同步,则单向时延测量会有很大的时钟误差。

网络分组的时延 D_{total} 是一个随时间变化的随机变量,由固定时延 D_{fix} 和可变时延 D_{var} 两部分构成。固定时延 D_{fix} 是基本上不变的,它由传播时延 d_p 和传输时延 d_{tran} 构成。传播时延 d_p 由固定的物理传输介质确定并且是固定的。传输时延 d_{tran} 由分组大小和链路的容量决定,一个分组的大小一旦固定,通过的链路容量便是固定的,其传输时延 d_{tran} 也是固定的。因此分组时延 D_{total} 可以用公式(1)描述:

$$D_{total} = D_{fix} + D_{var} = d_p + d_{tran} + D_{var} \quad (1)$$

固定时延可以看成与分组大小成线性的关系。假设网络入口和出口之间由 N 条链路构成,第 i 条链路的容量为 C_i,分组的大小为 s,链路 i 的传播时延为 d_p^i,则固定的时延可以用公式(2)描述:

$$D_{fix} = \sum_{i=1}^{N}(d_p^i + s/C_i) = s\sum_{i=1}^{N}1/C_i + \sum_{i=1}^{N}d_p^i \quad (2)$$

分组时延中的可变时延是由很多因素造成的。它可以分成中间路由器处理时延和排队等待时延两部分。对于任何一个分组,中间路由器总要对其进行路由查表以确定其转发端口,这个时间可以看成是处理时间。同时,中间路由器繁忙可能导致分组排队等待处理,也需要一段等待时间。处理时间和等待时间是不固定的,由路由器的具体性能以及链路的拥塞状况而定,是一个随机变量。所以如果链路不出现拥塞,一个分组的最小时延便与该分组的大小成线性关系。

从上面对时延构成的分析可以看出,分组的时延具有突发性和偶然性,为了能够使测量结果尽可能地反映网络的真实情况,可以采用低通滤波的方法来消除随机性。同时,对于单向时延测量要求时钟同步这一点在实际的测量中很难做到,因此许多测量方案采用返程测量,根据返程测量的结果来衡量单向时延,以避开时钟的同步问题。具体的测量算法是:入口路由器将检测包打上时戳后,发送到出口路由器。出口路由器一接收到检测包便打上时戳,随后立即使该数据包原路返回。入口路由器接收到返回的数据包后就可以评估路径的端到端时延 D。更新平均时延 D_{avg} 可以用公式(3)描述:

$$D_{avg} = (1 - \xi) * D_{avg} + \xi * D \tag{3}$$

其中,ξ 为平滑因子,是一个固定常数,一般为 0.1~0.2。

2.2 测量过程中"噪声"分组的过滤

采用主动测量时,难免受到"噪声"分组的影响,所谓"噪声"分组指夹杂在探测分组当中,或处于探测分组之前、之后对测量结果造成影响的业务分组。例如采用分组对(Packet pair)或多分组(Multi - packet)技术测量链路的瓶颈带宽时,难以保证探测分组在瓶颈链路处彼此相邻排队,可能会在中间插有其他分组,导致时间扩展(瓶颈带宽低估),或经过瓶颈链路后在第一个分组前插入其他分组,导致时间压缩(瓶颈带宽高估)。使得时间压缩和时间扩展的分组就是测量过程中的"噪声",怎样消除这个噪声?可采用的方法有:(1)求均值,但是由于"噪声"的随机性,该方法会造成较大误差;(2)在带宽估计的分布值中,选择密度最大的点,如采用直方图统计技术,但是事先不知道带宽的分布情况,直方图的条(bin)的宽度不好给;(3)采用在统计学中使用的非参数估计方法——核密度(kernel density)估计算法[7]。

定义核函数 $K(t)$

$$\int_{-\infty}^{+\infty} K(t)\mathrm{d}t = 1 \tag{4}$$

在任一点 x 的密度为

$$d(x) = (1/n)\sum_{i=1}^{n} K((x - x_i)/(c \cdot x)) \tag{5}$$

式中,c 是核宽度比,n 是 $c \cdot x$ 内 x 的点数($h = cx$ 是核宽度,n 是宽度 h 内 x 的点数),x_i 是测量得到的第 i 个带宽值。

核函数可选为

$$K(t) = \begin{cases} 1 + t, & t \leqslant 0 \\ 1 - t, & t > 0 \end{cases} \tag{6}$$

对于发端两分组的间隔不是足够小的时候,密度估计函数会失效,为此引入一个收发带宽比的参数,即收端和发送带宽 $s(x)$ 的比:

$$p(x) = 1 - [\ln(x)/\ln(s(x))] \tag{7}$$

假如两个采样点(接收带宽)有相同的发送带宽,则 $p(x)$ 偏重于接收带宽较小的那一个,为了解决这个问题,定义接收带宽比

$$r(x) = [\ln(x) - \ln(x_{min})]/[\ln(x_{max}) - \ln(x_{min})] \tag{8}$$

这样过滤函数为

$$f(x) = a \cdot [d(x)/d(x)_{max}] + b \cdot p(x) + c \cdot r(x) \tag{9}$$

使 $f(x)$ 为最大值的 x 为瓶颈链路带宽。问题在于如何选取最佳的过滤函数的系数 a,b,c 的值。

2.3 丢包率测量

许多因素会导致数据包在网络上传输时被丢弃,例如数据包的大小、数据包在什么时间发送(链路是否拥塞)等。大的数据包肯定比小的数据包容易丢失,链路拥塞情况下发送的数据包也容易丢失。

为了评估网络的丢包率,一般采用直接发送检测包来进行测量。但是发送检测包测量丢包率需要一定的数据模型,否则无法进行准确的评估与预测。目前评估网络丢包率的模型有3种:贝努利模型、马尔科夫模型和隐马尔科夫模型。贝努利模型假定每个数据包在网络上传输时被丢的概率是不相关的,因此它比较简单而且计算的复杂度不高,但其预测的准确度以及可靠性都不太理想。马尔科夫模型认为连续的数据包被丢弃的概率具有一定的相关性,但要求对链路的状态有清晰的了解。而在实际网络中,链路的状态是不容易被正确测量的,总是具有一定的随机性。因此,马尔科夫模型具有一定的局限性。隐马尔科夫模型修正了马尔科夫模型的缺陷,但是该模型得到的估计值很可能是局部最优,而不是全部最优。此外,马尔科夫模型的一个问题就是收敛比较慢,这对实时测量来说是不可以忍受的。相关的分析表明,基于马尔科夫模型的丢包率测量器收敛速度至少在秒级。因此,寻找适合网络测量的快速收敛算法是进一步发展该模型必须要做的工作。

2.4 时钟偏移影响的消除

网络测量的精度主要受测量方法或算法的影响,非合作测量还受网管的干预、网络安全机制、被探测方采取防探测的方法等因素的影响。多点合作进行端到端测量时,收发端时钟不同步成为误差来源之一。Vern Paxson 利用在一对节点之间进行正向、反向时延测量来确定收发时钟的误差,包括相对偏移(relative offset)和频差(skew)。后来又有人采用线性回归算法(linear regression algorithm)、分段最小算法(piecewise minimum algorithm)来消除时钟的不同步的影响,Sue B. Moon 等提出了基于线性规划的算法(linear programming),测量和仿真表明线性规划算法与其他算法相比,快速、稳定且易实现[8]。此外还有其他许多问题,如网络测量和分析中的抽样问题(建议采用增量随机抽样,如 Poission 抽样等)、统计方法的应用等。

3 结束语

网络测量涉及对网络各种参数的测量。文中就时延测量、"噪声"分组的过滤、丢包率的测量以及时钟偏移影响的消除进行了分析。探讨了各种测量模型以及存在的

(下转第104页)

改进算法主要是针对减少候选项的数量、及跳过对于频繁项目集产生无贡献的记录的考虑而获得性能改进的。当数据库包含的项数较少时,通过连接操作产生的候选项数也较少;当数据库规模较小时,扫描数据库过程中忽略的记录也较少,所以在这种情况下,由于整个挖掘过程的所耗费的时间较少,从而改进算法的效率提高不明显。

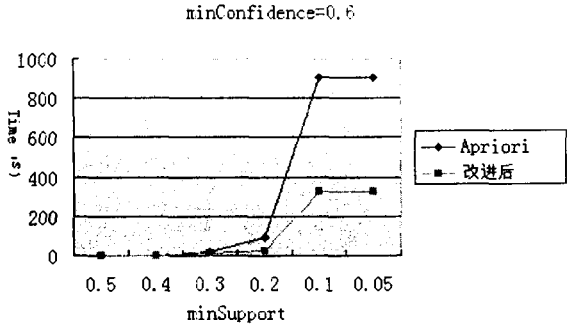

图 1 两种算法在不同支持度下的时间性能比较

4 小 结

文中对关联规则挖掘的经典算法 Apriori 算法进行了讨论分析,研究了相关的性质,提出从减少候选项数及减少实际需要考虑的交易记录数的角度改进挖掘算法的思想,并通过实验证明了改进方法的有效性与正确性。

关于关联规则挖掘研究的下一步研究方向可以是研究面向分布式环境下的关联规则挖掘问题,研究结合背景知识的关联规则挖掘问题。

参考文献:

[1] Han Jia Wei, Kamber M. Data Mining - concepts and techniques[M]. San Francisco, CA: High Education Press, Morgan Kaufman Publishers, 2001.

[2] Frawley W J, Piatetsky G, Shapiro C, et al. Knowledge Discovery in Databases: An Overview[A]. In: Piatetsky - Shapiro, Frawley W J. Knowledge Discovery in Databases[C]. Menlo Park, California: AAAI Press/The MIT Press, 1991. 1 - 27.

[3] Fayyad U, Piatetsky - Shapim G, Smyth R. From Data Mining to Knowledge Discovery: An Overview[A]. In: Fayyad U. Advances in Knowledge Discovery and Data Mining[C]. Menlo Park, California: AAAI Press, 1996. 1 - 34.

[4] Uthorosamy R. From Data mining to Knowledge Discovery: Current Challenges and Future Directions[A]. In: Fayyad U. Advances in Knowledge Discovery and Data Mining[C]. Menlo Park, California: AAAI Press, 1996. 561 - 569.

[5] Agrawal R, Imielinski T, Swami A. Mining Association Rules Between Sets of Items in Large Databases[A]. In: Proceedings of 1993 ACM - SIGMOD International Conference Management of Data(SIGMOD'93)[C]. Washington D. C.: [s. n.], 1993. 207 - 216.

[6] Agrawal R, Srikant R. Fast algorithms for mining association rules in large database[R]. Technical Report FJ9893, San Jose, CA: IBM Almaden Research Center, 1994.

[7] Agrawal R, Srikant R. Fast algorithms for mining association rules[A]. In: Proc of 20th Int Conf Very Large Databases (VLDB'94)[C]. CA: [s. n.], 1994. 487 - 499.

[8] 徐 瑞,乔志萍,李伟华. 单维关联规则快速 Apriori 算法研究[J]. 微电子学与计算机,2005,22(2):43 - 45.

[9] 王创新. 关联规则提取中对 Apriori 算法的一种改进[J]. 计算机工程与应用,2004(34):183 - 185.

[10] XU Yong, Zhou Sen - Xin, Gong Jin - Hua. Mining Association Rules with New Measure Criteria[A]. In Proc of the 4th Int Conf of ICMLC[C]. [s. l.]: [s. n.], 2005. 2257 - 2260.

[11] 李清峰,杨路明,张晓峰,等. 数据挖掘中关联规则的一种高效的 Apriori 算法[J]. 计算机应用与软件,2004,21(12):84 - 86.

(上接第 101 页)

问题。同时由于网络快速发展,新应用不断提出,网络正变得越来越复杂。为了应付日益复杂的网络,必须提出新型的网络测量方案,为整个网络稳健、可靠、高效运行提出依据。文中正是在这种背景下详细讨论了网络测量中的关键技术,为其进一步的发展打下基础。

参考文献:

[1] Paxson V, Floyd S. Wide - area traffic: the failure of poisson modeling[J]. IEEE/ACM Transactions on Networking, 1995, 3(3): 226 - 244.

[2] Real Time Flow Measurement Working Group[EB/OL]. http://www.ietf.org/html.charters/rtfm - charter.html, 2002.

[3] Mahdavi J, Paxson V. IPPM Metrics for Measuring Connectivity, RFC2678 [EB/OL]. http://www.ietf.org/rfc/rfc2678.txt, 1999 - 09.

[4] Paxson V. Measurement and Analysis of End - to - End Internet Dynamics[D]. Computer Science Division, University of California Berkeley, 1997.

[5] Almes G, Kalidindi S, Zekauskas M. A One - way Delay Metrics for IPPM, RFC2680[EB/OL]. http://www.ietf.org/rfc/rfc2680.txt, 1999 - 09.

[6] Almes G, Kalidindi S, Zekauskas M. A Round - trip Delay Metrics for IPPM, RFC2681[EB/OL]. http://www.ietf.org/rfc/rfc2681.txt, 1999 - 09.

[7] Lai K, Baker M. Nettimer: a Tool for Measuring Bottleneck Link Bandwidth[DB/OL]. http://mosquitonet.stanford.edu/laik/, 2001.

[8] Moon S B, Skely P, Towsley D. Estimation and Removal oF Clock Skew from Network Delay Measurements[A]. proceedings of IEEE INFORCOM99[C]. New York, USA: IEEE, 1999. 227 - 234.