Internet 网络测量方式综述

牛燕华[1,2] 任新华[1] 毕经平[2]

[1](太原理工大学网络信息中心 山西 太原 030024) [2](中国科学院计算技术研究所 北京 100080)

摘 要 随着网络规模的迅速膨胀及其复杂性的增加,网络测量受到越来越多的重视。根据测量方式,可把网络测量分为主动测量和被动测量两大类。对这两类测量方式的原理及各自的优缺点分别阐述并进行比较,特别强调了采用每种测量方式所需注意的安全问题,同时剖析了国内外相关领域的研究现状,并通过一个实例具体讲述这两种测量方式在实践中的应用。

关键词 网络测量 主动测量 被动测量 FOX

A SURVEY ON INTERNET MEASUREMENT MODE

Niu Yanhua[1,2] Ren Xinhua[1] Bi Jingping[2]

[1](*Network Information Center, Taiyuan University of Technology, Taiyuan Shanxi 030024, China*)

[2](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China*)

Abstract With Internet expanding in quantity and complexity, network measurement becomes more and more important. According to measurement mode, network measurement could be classified into the following two categories: active measurement and passive measurement. In this paper, the principles of the two measurement modes are explored. The strong and weak points are given. The security aspects are accentuated. The development of the relative research field is introduced. And the theory is expatiated through an exact example.

Keywords Network measurement Active measurement Passive measurement FOX

1 引 言

伴随着飞速增加的带宽、实时和多媒体应用的普及、几乎持续地以指数规律增长的规模,Internet 的控制机制和行为特征日趋复杂和难以理解。为了认识和理解现代互联网络的行为特征和性能表现、保证和提高现有网络服务质量、推动互联网和信息基础结构的健康发展,研究 Internet 网络测量势在必行。

测量网络的拓扑结构,对网络结构进行动态描述,并根据网络的变化分析网络的性能,对网络效率和行为做出评价,它有以下几方面的应用:

- 网络监视;
- 流量描述;
- 网络质量控制和辅助性网络管理;
- 防范大规模网络攻击,同时为信息攻击对抗提供必要的网络测绘和流量分析;
- 对不同 ISP(Internet service provider)的 QoS 的比较、移动 IP 的位置发现、代理服务器的自动选择等许多方面;
- 为仿真模拟 Internet 环境、协议设计与评价以及动态网络存活性分析提供研究基础;
- 为 Internet 流量工程和网络行为学的研究提供基础辅助依据及验证平台。

网络测量的分类标准有多种。比如,根据测量方式,可以分为主动测量和被动测量;根据测量基准,可以分为基于流、基于网络接口、基于连接、基于节点对和基于路径的网络测量;根据测量点的多少,可分为单点和多点测量;根据被测量者是否知情,可分为协作式测量与非协作式测量。

本文重点介绍网络测量方式,即主动测量和被动测量。

2 主动测量

2.1 主动测量方式的测量原理

主动测量[1,2]是由 AMP(Active Measurement Project)组织提出的数据分析方法。这种测量方式实际上就是映射 Internet 系统,在主动测量方式中,通过向网络中发送数据、观察结果和发送数据所需时间来研究网络的行为。主动测量本身产生新的业务测量流量,利用这些业务量测量反映网络提供给其他用户的服务的参数,包括 round-trip time(RTT)和丢包率等。这些测量流量可能会引起网络的特殊响应(如 traceroute),或网络为流量提供某种性能(如 treno)。在主动测量过程中,测量流量可通过详细定义,在一定的控制条件下产生。

主动测量是基于 RTT 测量,而不是对单程延迟的测量。因为 RTT 测量更易于实现,而且不会依赖外部设备去同步两台监视器的时间。另外,有的测量方法是使用全球定位系统(GPS)接收器来同步主机的时间。但是这些系统过于昂贵而且难于安装,并且获得的额外信息也很有限,因此并不普及。

收稿日期:2004 - 03 - 15。本文受国家自然科学基金(90104006)和国家 863 计划(2001AA112135)的支持。牛燕华,硕士生,主研领域:网络测量与分布式系统应用研究。

具体来说,RTT 测量是通过类似 Ping 的程序,每隔一定时间段进行一次。该程序对每台被测主机发送 ICMP 响应包,然后等待 ICMP 的回应包,记录每个站点的测量延迟。发现或者诊断一个站点故障的最好方法之一就是查看 RTT 图标的起伏状况,这些起伏表明了路由或者配置上的变化所引起两个站点间 RTT 的改变情况。

另外一点,就是要查看丢包率。如果一个站点的丢包率过高,那么它可能出现硬件损坏,这种分析是非常基本的。如果要对一个站点的性能有进一步理解,就要通过比较它同其他站点的连通性来获得。比如,被测站点日常链路出现的拥塞是否也同样出现在其他站点上?连接回程时间是多少?

2.2 主动测量的优缺点

主动测量的优点如下:

- 使用方便,适合端到端的网络性能测量,对于需要关心的内容只要在本地发送测试包观察网络的响应即可;
- 由于该方法不涉及用户的网络信息,所以对用户而言是很安全的。

但它也存在一定的缺点,主要包括:

- 它增加了网络潜在的负载,尤其是如果该测量未经仔细设计,使产生的流量达不到最小,可能会对网络造成较大的影响;
- 主动测量会引起 Heisenberg 效应,即额外的流量可能会干扰网络,并使结果分析产生偏差。

另外,需要注意的是,在同样都是主动测量的情况下,一些测量工具可能会比其它测量工具‘更加’主动一些,如 Ping 程序在执行过程中只对网络带来较轻微的负载,所以 Ping 测量因 Heisenberg 效应带来的偏差比上述瓶颈带宽的测量要小得多。

2.3 主动测量中的安全问题

对于主动测量技术,需要将测试流量注入网络,这种测试流量有可能会影响网络的拥塞情况,因此要谨慎地控制所用的测试流量,避免因测试而引起网络拥塞[3]。另外,要避免主动测量技术被滥用,如利用此技术进行伪造测试流量的拒绝服务(DoS)攻击。

2.4 国内外关于主动测量的研究进展

到目前为止,人们所做网络测量项目中的大多数都涉及到主动测量。到了 2000 年 6 月,运行主动测量监视器的源站点有 116 个(美国 114 个,新西兰、挪威各 1 个),被测量的目的站点约有 13340 个。到了 2003 年 11 月,运行主动测量监视器的源站点已增加到 140 多个。其目的是为了增强参与站点和用户对高性能网络运行情况的理解,帮助网络用户和网络服务提供者分析问题。

美国的 NIMI(National Internet Measurement Infrastructure)项目[4],利用 ping,tracerute,mtrace 等工具进行主动测量,它是一个可进行大规模网络测量的测量基础设施,创建了一个通用的架构,具有良好的可扩展性。NIMI 的主要特点在于它不是为某种特殊的分析目标执行特定的测试集,而是可以灵活地在底层架构之上添加自己所需的测量工具。

NLANR(The National Laboratory for Applied Network Research),NAI(Network Analysis Infrastructure)是美国的一个研究支持 HPC(High Performance Connection)的组织建设的基础设施[5]。与其它项目相比,NIANR 主要有以下两个特色:1)数据收集方式全面,包括主动、被动和控制监视;2)数据可视化采用了三维形象显示的方式。

Surveyor[6] 是一个建立在全球参与站点上的测量平台,部分由 NSF(National Science Foundation)支持。它测量 Internet 的路径性能,包括单向延时、损耗、路由测量等,并研究相应的分析方法与工具。Surveyor 的特色主要表现在 1)采用标准的测试方法,使得结果具有可比性;2)利用 GPS 卡进行时钟同步,对于单向的测量准确率较高。

依托于 UCSD/SDSC(University of California,San Diego,Supercomputer Center)的研究部门 CAIDA[7](Cooperative Association for Internet Date Analysis),开展网络测量、分析、可视化工具的研发,维护全球因特网平台的健壮性和可扩放性,受到 NSF、DARPA(Defense Advanced Research Projects Agency)、ISP 和硬件供应商的资助,研究对象包括 Internet 拓扑结构、网络负载、网络性能、网络路由、监测正、异常活动,关注带宽估计、负载刻画、长期趋势识别,以进行流量工程设计、能力计划、安全迹象检测等等。

Skitter[8] 是一个采用主动测量方式来测量一系列主机的转发路径和 RTT 的工具。Skitter 选用了较多的被测节点,与其它项目相比,该项目测量范围大,对 Internet 的覆盖面要广得多。

加拿大国家研究机构使用 perl script 跟踪对 TRIUMF 感兴趣的节点,每 10 分钟检测一次丢包率,每天收集 4 次 tracert 数据并生成网络可视化图[9];欧洲的 PPNCG(Particle Physics Network Coordinating Group)项目,监视全欧洲某些粒子物理研究所的网络端到端性能,并加以优化[10]。

国内的国防科学技术大学、西南交通大学等单位在基于 ICMP 协议的 IP 拓扑探测方面的技术比较成熟;哈尔滨工业大学计算机科学与工程系实现了一个大规模网络拓扑测量的原型系统,能够针对大规模网络进行路由 IP 拓扑结构的自动发现,并进行可视化显示;中国科学院计算技术研究所信息网络室开发出大规模 INTERNET 网络测量与分析系统 NIPMAS,该系统能对跨地域的大型网络进行在线监测,并能根据用户需求灵活添加业务测量工具,实现对网络主要性能状态的监测,分别针对网络业务运行正常、亚健康状况(即网络设备正常但业务运行不正常)和用户业务完全不能进行(即网络设备或链路不正常)状态进行了具体性能监测或故障定位,另外,NIPMAS 还实现了 GIS 显示、动态播放和 Web 发布等功能;在 NIPMAS 的基础上,中科院计算所还开发出支持 IPv6 的大型网络测量系统 FOX,在国内外处于领先地位。

3 被动测量

3.1 被动测量的测量原理

与主动测量相对应的是被动测量[11],在被动测量方式中,记录网络活动的探针被接入到网络中的某个点上,在大多数情况下探接到网络节点之间的连接上,然后使用包过滤器捕获通过该点的数据包,汇总和记录那条连接上业务流量的信息。因为包过滤能够捕获网络流量而不会对网络造成什么影响,所以使用被动测量可以消除额外的流量负载和 Heisenberg 效应。

被动测量使用设备监视经过它的流量,这些设备可以是专用的(如 Sniffer),也可以是嵌入在其它设备(如路由器、防火墙、交换机和主机)之中的(如 RMON,SNMP 和 netflow[12] 使能设备等)。测量软件或系统周期性地轮询被动监测设备并采集信息

(在 SNMP 方式时,从 MIB 中采集),以判断网络性能和状态。

3.2　被动测量的优缺点

被动测量的优点如下：

- 在测量时并不增加网络上的流量,测量的是网络上的真正流量；
- 能够达到对观察点网络行为的详尽理解；

但它也有其本身所固有的缺点：

- 关于隐私和安全的问题：被动测量方式可能要查看网络上的所有数据包,容易捕获网络中的敏感信息,给用户信息的保密和安全带来一定威胁；
- 只能获得网络局部数据,无法了解网络整体状况或对网络的端到端行为的理解：被动测量只能固定在网络的某一点收集数据,而不能根据网络的整体情况来调整收集策略；
- 被动测量在网络排错时特别有价值,但在仿真网络故障或隔离确切的故障位置时会受到限制；
- 被动测量的前提是协作,否则无法在测量点安装必要的软、硬件设备,测量范围由此而受限。

3.3　被动测量中的安全问题

对于被动测量技术,由于需要采集网络上的数据包,因此会将用户数据暴露给无意识的接收者,对网络服务的客户造成潜在的安全问题。所以,在进行被动测量时,要尽量避免对用户数据载荷的分析,并适当降低采样速率,以最大限度地保护用户数据。解决这些相关问题的一个主要方法是编写只捕获数据包中与内容不相关的部分字节的程序,使用这样的程序进行被动测量,可使隐私和安全问题得到很大程度的保障。

3.4　国内外关于被动测量的研究发展

目前开展的被动测量项目有：受 NSF 资助的美国应用网络研究国家实验室(NLANR)的测量项目 PMA(Passive Measurement and Analysis),它主要进行基于包头追踪的分析,另外还有来自于参与 PMA 项目服务器的 SNMP 信息和基于 BGP 数据的分析,旨在为高级网络(如 vBNS,Abliene)提供协作性的服务支持。它采用 OC 3mon 数据搜集系统,包括专门的群机系统、装有 FORE ATM cards 和 Optical Splitters(分光器),采集 ATM 的数据流,使用 CoralReef 根据一定的规则集进行数据采集,并可使用 perl 等语言分析数据[13]。

Berkeley University 和 IBM 共同开发的 SPAND(Shared Passive Network Performance Discovery)项目[14],通过对捕捉到的 UDP/TCP 分组进行分析得到连接带宽、丢包率等性能。

Fluke 公司开发的 SuperAgent[15] 在不增加网络负荷的基础上,测量应用程序响应时间并分解至网络、服务器和应用程序部件。它可以连接至交换机镜像端口或服务器组群附近的网络在线监测接口盒,根据实时的应用程序流量检查 TCP 数据包头信息。SuperAgent 将测量结果保存在一个可以通过基于 Web 的界面访问的 SQL 数据库中。它还通过电子邮件提供报告和报警,或利用一个已有的管理系统。利用 NetQoS 的 Reporter-Analyzer,可以将 SuperAgent 信息与来自其他来源的信息组合在一起。

国内中科院计算所信息网络室开发的 NIPMAS 和 FOX 也可嵌入被动测量工具来开展被动测量。

4　大型网络测量系统 FOX

FOX 是中科院计算所信息网络室网络测量与分析课题组研究开发的支持 IPv4/v6 测量和分析系统。该系统主要具有以下功能：1)对 IPv4/v6 网络的网络层性能进行监测,包括对网络延迟、丢包、吞吐量等性能参数的准确测量；2)对 IPv4/v6 网络的应用层性能监测,可以对 HTTP、E-Mail、FTP 和 TELNET 等多种应用进行测量；3)由于在设计过程中充分考虑了系统的可扩展性,FOX 系统不仅支持主动测量,也可支持被动测量,只要在系统中添加被动测量工具,就可以方便地进行被动数据的获取；4)监测数据的灵活分析,系统可利用收集到的数据进行灵活分析,既可支持数据格式的灵活性,又可支持分析方式的多样性,同时还在系统中内嵌了 Excel 和 SPSS 等强大的分析工具辅助测量数据的分析。

FOX 主要由控制中心、测量探针和分析平台三大模块组成。控制中心负责测量任务的调度、测量结果的回收等指挥工作；测量探针接收任务命令、具体展开测量、并把测量得到的结果送到数据分析平台；分析平台过滤数据、绘制图表、提供给用户反映网络运行状况的直观的测量结果显示。

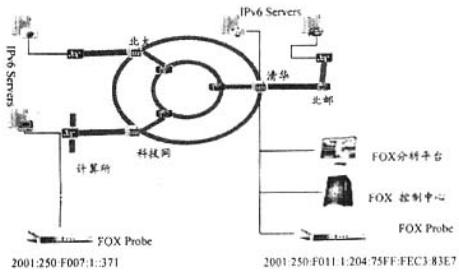

图 1　FOX 测量装置部署示例

图 1 所示为 FOX 系统的测量装置部署示例,测量 IPv6 科技网的试运行情况。控制中心和分析平台都设在清华大学,在清华大学和中科院计算所分别安装测量探针。

首先讲述主动测量。如果想了解从计算所通过此试验科技网访问北邮的 Web 服务器的情况,则采用主动测量方式非常合适。计算所探针模拟实际用户访问北邮的 Web 服务器,由探针上所安装的 HTTPv6 测量工具向被测服务器发起连接请求、构造 HTTP 信息包,模拟实际用户,完成一次测量。在探针和服务器的交互过程中,记录和计算有用的数据,从而得到连接时间、下载页面的时间、HTTP 业务吞吐量等指标。主动测量会给网络增加一定的负担,但它对于评测实际用户对网络服务的感受非常有效。

被动测量的工作方式与主动测量截然不同,适用范围也不同。如果想了解某一时刻或某段时间内通过清华大学主干网的流量,则在如图 1 所示的清华大学节点探针上安装被动测量工具,被动测量不构造数据包,而是监听每一个经过的数据包并记录下来进行分析,对于评估网络的吞吐量非常有效。

无论是主动测量,还是被动测量,控制中心一视同仁。根据用户需要通过发送命令让探针以周期方式或主从方式工作,测量得到的数据返回给分析平台。用户通过分析平台处理的结果可以直观快速地了解网络性能和业务情况。

5　结束语

Internet 已成为人们日常生活不可缺少的一部分,随着其迅猛发展,网络测量越来越重要。网络测量为加强网络管理、提高网络利用率、防范大规模网络攻击提供了技术平台,是一个具有

(下转第 25 页)

Agent的通信机制。Agent 获取信息的途径主要有查询、预订、传递和中介四种[8],本文采用传递的方式实现了它们的通信。

4　数据汇聚与发布服务的实现

"苏州市古城区水环境实时监控系统"采用的编程语言是 Java,数据库服务器是 Oracle 9i 数据汇聚与发布服务采用的 SOAP 引擎是 Axis1.1。

为了让 Axis 知道发布的服务,需建立 server-config.wsdd 文件,此文件的部分代码如下:

```
<?xml version="1.0" encoding="UTF-8"?>
<deployment xmlns="http://xml.apache.org/axis/wsdd/"
  ……
  <service name="RelesIntegnData" provider="java:RPC">
    <parameter name="allowedMethods" value="*"/>
    <parameter name=
      "className" value="webdata.RelesIntegnData"/>
  </service>
  ……
</deployment>
```

文件中发布了一个 RelesIntegnData 服务。以下是调用此服务的一个 GUI 截图,如图 3 所示。

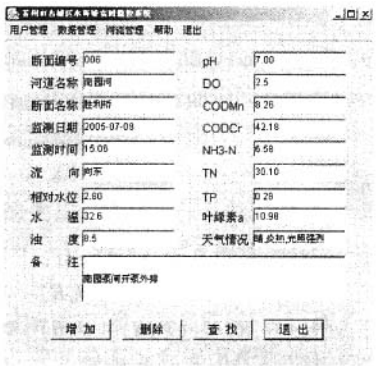

图 3　数据汇聚与发布服务调用界面

在调用数据汇聚与发布服务时,客户层提供的参数作为 SOAP 消息的一部分被传入。数据汇聚与发布服务根据参数信息决定给客户层提供相应的服务。其调用机制如下:

```
Service service = new Service();
Call call = (Call) service.createCall();
call.setTargetEndpointAddress(new java.net.URL(endpoint));
call.setOperationName(method);
call.invoke(new Object[]{});
```

5　结　论

本文针对"苏州市古城区水环境实时监控系统"对水环境数据进行汇聚与发布的迫切需求,提出了相应的解决方案,并成功地解决了因不同测试方法与监测仪以及同一监测项具有多个数据源所带来的问题。重点提出了数据汇聚与发布服务,采用了先进的智能 Agent 和 Web 服务技术,使数据处理过程具有自治性和反应性,服务具有开放性、可扩展性和可移植性等优点。数据汇聚与发布服务与系统中其它模块间的无缝集成,充分发挥了各个模块的功能优势。此模型可推广到系统的整个领域(包括其他类似应用)。

参　考　文　献

[1] 国家环境保护总局、国家环境监督检验检疫总局,地表水环境质量标准(GB3838-2002),2002.

[2] 国家环境保护总局,地表水和污水监测技术规范(HJ/T91-2002),2002.

[3] 国家环境保护总局,景观娱乐用水水质标准(GB 12941-91),1991.

[4] 薛朝霞等,"引水冲污治理苏州的水环境",《中国给排水》,2002,Vol.18.

[5] Wooldridge M, Jennings N R. Intelligent Agents: Theory and Practice. Knowledge Engineering Review, 1994, 10.

[6] 杨芙清、梅宏、吕建等,"浅论软件技术发展",《电子学报》,2002,30(12A):1901~1906.

[7] 奚旦立、孙裕生、刘秀英,环境监测,高等教育出版社,1994.3.

[8] 陈海龙,多 Agent 系统通信策略研究,中国科技论文在线 http://www.paper.edu.cn.

(上接第 13 页)

重要理论研究价值和广泛的实际应用背景的课题。所有的互联网管理者、运营者和使用者都将从中获益。

参　考　文　献

[1] Vern Paxson, Andrew Adams and Matt Mathis, Experiences with NIMI. In proceedings of Passive and Active Measurement, 2000.

[2] Attila Pásztor and Darryl Veitch, A precision infrastructure for active probing. In PAM2001, Workshop on Passive and Active Networking, Amsterdam, The Netherlands, 2001, pp. 33~44.

[3] Aditva Akella, Srinivasan Seshan and Anees Shaikh, An Empirical Evaluation of WideArea Internet Bottlenecks. In Internet Measurement Conference 2003. http://www.icir.org/vern/imc-2003/papers/p303-akella.pdf.

[4] Paxson V, End-to-End routing behavior in the Internet, IEEE/ACM Transactions on Networking, 1997, 5(5): 601~615.

[5] McGregor, H-W. Braun, J. A. Brown, The NLANR Network Analysis Infrastructure. IEEE Communications Magazine, Vol. 38(5): pp. 122~128, May 2000.

[6] Kalidindi S, Zekauskas MJ, Surveyor: an infrastructure for Internet performance measurements. In Proceedings of the INET'99. San Jose, 1999. http://www.isoc.org/inet99/proceedings/4h/4h_2.htm.

[7] Claffy K, Monk TE, McRobb D, Internet tomography, Nature, 1999, January 7. http://www.nature.com/nature/webmatters/tomog/tomog.html.

[8] Bradley Huffaker, Marina Fomenkov, David Moore and kc claffy Macroscopic analyses of the infrastructure: measurement and visualization of Internet connectivity and performance. http://www.caida.org/tools/.

[9] http://www.triumf.ca.

[10] http://icfamon, rl.ac.uk/ppncg/title.html.

[11] Kc Claffy, Sean McCreary, Internet Measurement and data analysis: passive and active measurement. http://www.caida.org/outreach/papers/Nae/4hansen.html, 1999.

[12] Robin Sommer, Anja Feldmann, NetFlow: Information loss or win? In proceedings of The 2nd Internet Measurement Workshop, 2002. http://www.icir.org/vern/imw-2002/proceedings.html.

[13] http://moat.nlanr,net/.

[14] Srinivasan Seshan, Mark Stemm and Randy H. Katz, SPAND: Shared Passive Network Performance Discovery. In the Proceedings of the USENIX Symposium on Internet Technologies and Systems Monterey, California, December 1997.

[15] http://www.netqos.com/solutions/superagent/.