

Internet 测量基础架构的研究^{*}

Research of Internet Measurement Infrastructure

周轶刚 徐 莹

(北京航空航天大学软件开发环境国家重点实验室 北京100083)

Abstract With the Internet's ever-increasing size, it brings many problems such as network congestion and low quality of service, so strengthening network measurement and management has important influence on the development of the Internet. On the basis of analyzing the existent Internet measurement infrastructure, this paper points out their management and security problems, and then it proposes a new infrastructure solution.

Keywords Internet measurement, NPD, NIMI, IPMA

1 引言

随着现代信息技术的发展, Internet 及其各种应用构成了现代社会的重要信息基础设施。在 Internet 的发展过程中, 人们一直在对网络进行测量和控制^[5]。早期 Internet 将高可扩展性和强鲁棒性作为设计的主要原则, 当时网络应用较少且数据流量不大, 因此网络的测量和管理问题并不突出; 但是, 随着 Internet 规模的不断扩大, 人们经常遇到网络传输阻塞和服务质量低等问题, 所以加强对 Internet 的测量和管理, 进而提高网络运行的效益和质量是影响未来 Internet 发展的重要问题。

网络测量是一个笼统的概念, 是指通过设备和方法来测定与网络相关的物理或逻辑特性。目前, 对 Internet 网络的测量主要包含以下三个方面的内容:

- 网络拓扑探测^[9]: 通过主动发送 ICMP 包或 UDP 包, 对某一网段进行探测, 以得到此网段的大致拓扑结构和路由。

- 性能监测与分析^[9]: 通过监测网络的端到端的时延、抖动和丢包率等特性, 了解网络的可达性、利用率和负荷, 并发现网络瓶颈, 进而辅助解决网络问题。

- 网络的流量分析^[9]: 对网络“流”的特性进行测量和分析, 以掌握网络的流量特性, 比如协议的使用情况、应用的使用情况和用户的行为特征等。

一般而言, 在 Internet 上测量上述内容有主动测量、被动测量和基于 SNMP 的测量三种方法: 其中, 主动测量是通过向网络中注入测试流量数据, 并从中响应结果数据中获取网络状态参数, 代表性的主动测量软件有 Ping、Traceroute^[7]和 Iperf^[8]等, 它们主要用于测量网络的路由变化和可用的带宽; 被动测量是通过对网络流量及状态参数的监视和收集来完成测量任务, 代表性的被动测量软件有 TCPDump 和 NTOP 等, 它们可以按用户的要求记录相关的网络流量数据, 然后通过对记录的数据进行离线分析得到需要的结果; 基于 SNMP (简单网络管理协议) 的测量是指通过轮询的方式定期从支持 SNMP 的设备上获得网络的信息, 这种测量方式是随着 SNMP 协议的普及而流行起来的, 代表性的测量软件有 MRTG。在 Internet 上合理地使用上述三种测量方法, 就能够比较系统地刻画网络的运行状态和特征, 如获得网络拓扑结构、确定

网络的性能瓶颈和掌握网络应用的流量特性等, 并以此为基础对网络的设计、运行、管理、分析和规划提供有力的支持。

Internet 网络测量的本质是“端到端”测量^[2], 测量 Internet 这个松耦合的超大规模网络, 有范围广、内容多和变化大等特点。如果仅仅在有限的网络节点上运行特定测量工具, 只能反映局部网络在某个方面的网络特性, 因此, 为了使各种测量工具能够在整个 Internet 范围内工作, 需要一定的测量基础架构来支持测量工具的发布和运行、测量数据的采集和分析, 以及对自身的维护和控制。建立对 Internet 进行测量的基础架构, 基本要求是在网络节点上部署测量探测器——NPD (Network Probe Daemon)^[2], 这些探测器可以直接管理测量工具在该节点的运行。这些测量探测器是 Internet 测量基础架构中核心的元素, 它们通过相互合作和交互来支持复杂的网络测量过程。

本文在分析现有 Internet 网络测量基础架构的基础上, 针对其管理和安全问题, 提出了新的解决方案。

2 Internet 测量基础架构的需求

在复杂的 Internet 环境下, 建立适用且稳定的测量基础架构, 既要为各种网络测量工具和方法提供支持, 又不能影响网络的正常运行, 因此, 设计 Internet 测量基础架构, 有以下几点基本需求:

1. 异质网络适应性

Internet 是由异质网络硬件和软件组成的大规模松耦合网络环境。由于 Internet 只是强调网络的可连接性, 因此形成了大量硬件设备和软件协议各不相同的网络自治域, 这些自治域客观上形成了很多网络管理域, 不同的管理域有特定的管理方法、测量需求和测量策略, 这就要求测量基础架构能够适应不同管理域的特点。

2. 开放性

对 Internet 测量来说, 用很多不同的测量数据来评价网络的性能: 如 RTT (Round Trip Time)、路由、延迟和带宽等。但是对测量架构来说, 其立足点不是关注某种特定的网络数据, 而是提供支持大量不同类型测量的基础架构, 换句话说, 就是提供一个开放的平台, 能够方便地添加新的测量工具, 并稳定地承载各种测量工具共同工作。

^{*} 本文得到国家自然科学基金项目 (编号: 90104008) 的资助。周轶刚 莹 博士生, 研究方向为网络测量, 网络拥塞控制, 网络管理。

硕士研究生, 研究方向为网络管理, 网络测量, 软件工程, 分布式计算。徐

3. 可管理性和可控制性

设计 Internet 测量基础架构的本质问题是“谁将拥有、控制和维护测量节点”^[1]。如果由一个单一的组织来管理这个结构,显然不适合 Internet 的层次特性和分布特性,所以应该由网络的维护者自己来决定分布测量节点,并且有足够的管理功能和策略控制;同时,维护者手工管理小型规模的测量节点集合都是一个很棘手的问题,所以要提供能够减少管理的架构,这样可以使得整个测量架构可管理和可控制。

4. 安全性

Internet 测量架构是一个开放的平台,除了提供基本的测量服务以外,还提供允许各种新测量工具运行的接口,但是应该保证拒绝破坏性的测量工具,这就需要能够提供安全授权与安全验证机制,以保证测量平台和网络的安全性,以及测量请求和结果的准确性。

3 Internet 测量基础架构分析

3.1 NIMI

NIMI^[1](National Internet Measurement Infrastructure)是由美国先进网络研究国家实验室研发的一个网络测量项目。NIMI 没有任何测量工具所具有的测量知识,它致力于提供一个开放的允许大规模网络测量的基础架构,能运行并管理不同的测量工具来协助测量网络性能数据。

NIMI 强调构建可扩展的通用网络测量基础架构,而不是为了某个特定的测量或分析目的^[4]。NIMI 通过 NPD 来搭建一个通用的网络测量基础设施,用于测量 Internet 各个部分的全方位的、多精度的运行状况,并根据这些信息做出相应判断,以提高网络的性能,预测网络的行为。NIMI 如图3.1所示,其中主要有以下四种角色:

- 探测服务器 NPD(Network Probe Daemon):负责对测量请求权限校验、排队和执行测量请求。
- 测量客户端 MC(Measure Client):负责发送测量请求给探测服务器。
- 联系配置中心 CPOC(Configuration Point of Contact):作为一个管理节点和管理域内的 NPD 进行联系并对它们进行控制,如为 NPD 提供初始策略和更新管理策略。
- 数据分析中心 DAC(Data Analysis Center):对 NPD 返回的数据进行后处理功能的知识库服务器,能进行完整的测量数据统计和分析。

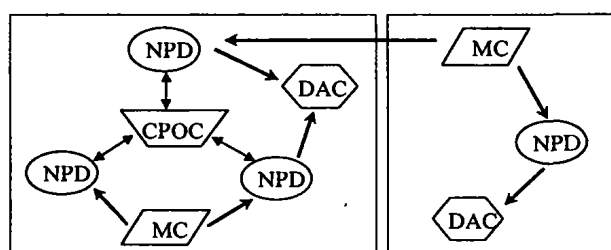


图3.1 NIMI 体系结构

其中,NPD 是 NIMI 架构中最重要的部分,它不仅是轻量级而且是可移植的,这样 NIMI 就可以部署在 Internet 中不同的软、硬件平台上;其次,NPD 的动态性使得测量节点的增加和调整非常容易;再次,NPD 的自配置特性使得对它的管理可以减少管理者的参与。在实现上,NPD 被分成三个主要部分:通信服务器、任务执行器和必须运行的测量程序的集

合,这样就能在满足基本测量和管理需求的基础上,同时保证新的测量工具能够不用修改就添加到 NIMI 中来。

可见,NIMI 体系结构不但彻底分离配置探针、请求测量、执行测量和分析结构这几个不同的任务,而且具有支持策略控制、本地管理和控制、保证测量安全和自动配置等特点,同时能够很容易地添加测量模块,基本满足了 Internet 测量基础架构的需求。目前,NIMI 已经部署在美国各大学和研究机构的35个网络测量节点上。

3.2 IPMA

IPMA^[6](Internet Performance Measurement and Analysis)是由美国密歇根州立大学电子工程和计算机系研发的一个网络测量项目。IPMA 项目的目标是开发测量工具来执行统计性的测量数据研究,以促进 Internet 的稳定和合理增长。

IPMA 项目研究的 Internet 统计量主要集中在以下两个方面:①路由稳定性,拓扑及其可视化;②提供网络性能测量数据;同时,IPMA 项目也致力于构建共享的 Internet 测量基础架构,其体系结构如图3.2所示,其中主要有五种角色:

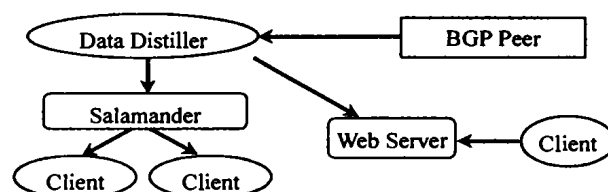


图3.2 IPMA 体系结构

- 边界网关协议对等体 BGP Peer:作为探测服务器,收集路由信息并复制到预先定义好的数据文件中。
- 数据分析服务器 Data Distiller:负责读取路由信息数据文件,并制成大量周期性报表。
- 发布服务器 Salamander(可选):负责将生成的报表发送给大量的报表订阅客户程序。
- Web 服务器 Web Sever:负责提供 Web 方式的报表浏览服务。
- 客户端 Client:可视化的浏览路由数据及丢包率、延迟等性能参数。

与 NIMI 不同,IPMA 测量基础架构是以测量具体网络性能数据为目标,其特点在于提供了一套完整的数据获取、数据分析、数据传送和数据表现的体系结构。

3.3 存在的问题

在 NIMI,IPMA 和其他网络测量项目的研究和实践过程中,出现了一些问题,研究这些问题有助于建立更完善的 Internet 测量基础架构:

1. 多使用主动测量方法,尽量不使用被动测量方法^[3]

被动测量需要在测量网络上运行测量平台或者测量工具,而这些平台和工具很容易成为木马程序的载体,从而给网络带来严重的保密和安全问题;此外,被动测量往往需要特殊的硬件和软件支持,使得被动测量程序的部署非常困难,所以多用主动测量而不是被动测量有利于整个测量基础架构的建立。

2. 最小化管理架构的负担

当运行状态的 NPD 突然遇到不可避免的错误时,如测量软件更新、包过滤错误配置和磁盘空间耗尽等,会造成系统崩溃、瘫痪或者重新启动,所以,在 NPD 中实现远程访问管理使软件能够自动更新,以及尽可能地加入自诊断功能,可以降低损

耗,提高系统稳定性。

3. 管理域边缘的防火墙屏蔽网络测量端口

出于安全考虑,一般商业网络在自治管理域的边缘设置防火墙来防止黑客攻击,而防火墙对非80端口数据包的屏蔽,客观上限制了各种网络测量工具的有效工作,同时也造成部署和运行 NPD 非常困难,所以应该提供某种机制使得能够基于 HTTP 协议进行网络测量,这样的测量基础架构才能真正在商业网络上部署并取得成功。

4 Internet 测量基础架构设计

在 NIMI 中,MC 的基本任务是向 NPD 发送测量请求和表示测量数据,但是在 Internet 上广泛分布 MC 给基础架构的管理和安全带来了问题:一方面大量的 MC 需要授权和认证加重了管理架构的负担,另一方面使得简单的风暴攻击就能造成基础架构瘫痪;此外,MC 所提供的局部和小量测量数据并不能给用户足够的信息。所以,可以分离发送请求测量和表示测量数据两种任务,即把 MC 分成测量请求客户端(MRC)和数据浏览客户端(DBC),其中,MRC 和 NPD 部署在相同位置构成测量探针平台(MPP),MPP 除了提供测量服务以外,同时也可以向别的 MPP 发送测量请求,这样既可尽量避免 NPD 受到风暴攻击,也可以减少对 MC 的管理负担;而 DBC 可以通过 Web 方式访问管理域数据分析中心(DAC),该中心定期采集自治管理域内所有 NPD 的性能测量数据,对这些数据进行计算整合后以 Web 报表的形式提供给用户,达到网络测量数据广泛共享的目的。这样,不仅解决了防火墙屏蔽测量端口的问题,而且可以实现测量数据的分布采集和测量结果的集中计算。

此外,在每个自治管理域中可以设置一个自治域管理中心(ASMC),该中心对管辖范围内的所有 MPP 进行管理,包括新测量工具的验证和发布以及调整管理策略等。

最后,完整的测量基础架构需要从全局的角度了解整个测量架构的情况,并且能够统一分析全网的测量数据。所以,设置一个 Internet 测量中心(IMC)采集 DAC 整合后的测量数据,来完成上述任务,而且可以对整个网络的测量数据进行综合评价和计算,并把结果通过 Web 方式发布,向网络用户提供当前整个网络的基本状况。

综上所述,改进后的 Internet 网络测量基础架构的体系结构如图4.1所示,其中

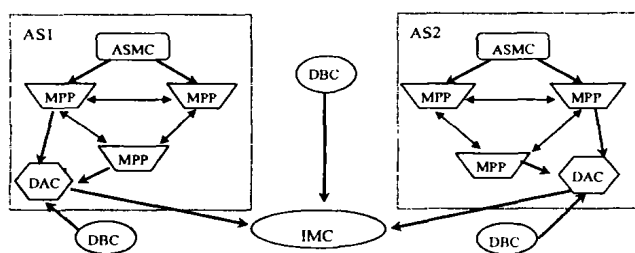


图4.1 改进体系结构

•测量探针平台 MPP:负责对测量请求权限校验、排队和执行测量请求,并向其余 MPP 发送测量请求。具备自我管理、自配置和动态处理管理策略的功能。

•自治域管理中心 ASMC:负责管理本管理域内的 MPP 并对它们进行控制,如为 NPD 提供管理策略和发布新测量工具等。

•数据分析中心 DAC:负责采集自治管理域内所有 MPP 的性能测量数据,进行完整的测量数据统计和分析,并把测量数据以 Web 报表的形式发布。

•Internet 测量中心 IMC:负责从各个 DAC 读取测量数据文件,计算整合后,以 Web 方式发布全网络基本状况,并为网络优化提供数据支持。

•数据浏览客户端 DBC:可视化的浏览 Internet 网络测量数据。

结论及展望 随着 Internet 规模的不断扩大,针对它的大规模测量研究工作变得越来越复杂,许多研究人员建议开发一个 Internet 测量基础架构,用来提供各种与网络运行有关的性能数据,并提供高质量、高有效性的网络测量和优化服务。本文研究了 NIMI 和 IPMA 等著名的网络测量项目,并根据它们存在的管理和安全问题,提出了改进后的网络测量基础架构,在该架构中,首先把测量客户端和测量探测器合并为测量探针平台,既减少了架构的管理负担,又尽量避免测量探测器受到风暴攻击;其次,通过层次化的测量数据处理、分析和发布,为网络用户提供了网络测量数据和性能指标。

我们下一步的工作是研制开发适合未来高速网络应用的测量方法和测量工具,如测量组播性能的工具等,并部署在网络测量基础架构中。

参考文献

- 1 Paxson V. An Architecture for Large-Scale Internet Measurement, 1998
- 2 Paxson V. Measurements and Analysis of End-to-End Internet Dynamics; [Ph. D. Thesis]. U. C. Berkeley 1997
- 3 Matthews W, Cottrell L, Salomoni D. Passive and Active Monitoring on a High Performance Research Network. 2001
- 4 Cottrell L. Comparison of some Internet Active End-to-end Performance Measurement projects. 1999
- 5 Adams A, et al. Creating a Scalable Architecture for Internet Measurement. 1998
- 6 Labovitz C, et al. The Internet Performance and Analysis Project. <http://www.merit.edu/ipma/docs/team.html>, 1997
- 7 Jacobson V, traceroute. <ftp://ftp.ee.lbl.gov/traceroute.tar.Z>, 1989
- 8 Tirumala A, Ferguson J. <http://dast.nlanr.net/Projects/Iperf/index.html>, Iperf Version 1.2, 2001
- 9 张慧勇,李纯喜,陈常嘉. Internet 网络流量的测量与分析. 通信世界, 2001. 7