基于 TCP/IP 的网络流量监测系统模型的研究

Research on Network Traffic Monitoring System Model based on TCP/IP

梁 鸿 刘 芳 (中国石油大学 计算机与通信工程学院 山东 东营 257061)

摘要:网络流量监测对网络的资源分布、容量规划、服务质量分析、错误监测与隔离、安全管理都十分重要,文中介绍了网络性能监测领域的研究现状,并在此基础上,提出了基于 TCP/IP 的网络性能监测模型,并阐释了实现该模型的关键技术。

关键词:流量监测 网络管理 自适应样本抽样

1 网络流量监测的意义

在过去的几十年里整个互联网发生了翻天覆地的变化。互联网的规模越来越庞大,结构越来越复杂。互联网络体系结构的复杂化使得网络的运行控制、管理维护、分析设计日趋困难。网络流量监测提供了一种在实际环境中探索网络特性的手段。网络流量监测是一个从网络设备上采集数据、解码数据、分析数据的过程。它从网络中采集一些具体的指标性数据,并反馈给监测者。这些数据对网络的资源分布、容量规划、服务质量分析、错误监测与隔离、安全管理都十分重要。

这些数据可以用来作为分析网络性能、了解网络运行动态、诊断可能存在的问题,甚至预测可能出现的问题。网络流量监测是网络管理和系统管理的一个重要组成部分,为网络的运行和维护提供了重要信息,对于网络性能分析、异常监测、链路状态监测、容量规划等方面发挥着重要作用,同时也是网络流量具体建模、分析的必要前提和手段。

2 网络性能监测

在此主要介绍网络性能的测量参数。网络流量的测量实体包括流量大小、传输时延、包丢失率、包误差率。

2.1 流量大小

包括均值、抖动变化,可以根据不同的聚合层次来考察:IP 地址、接口、链接、节点、节点对、路径、网络边缘、用户、自治系统。

2.2 IP 包传输时延

IP 包传输时延定义为穿过一个或多个网络段,传送 IP 包所经历的时间(不考虑传送成功与否)。时延,通常是指由于网络节点处的路由器处理网络数据流量时所产生的时延,可以反映出路由器的包的排队时延,而一个节点对之间的时延则可以反映出该网络路径上的单向时延。

2.3 IP 包丢失率

IP 包丢失率是丢失的 IP 包传送结果与所有 IP 包的比值。导致分组丢失的原因有网络故障/协议错误引起的丢失和网络审查引起的丢失。

2.4 IP 时延变化(即抖动)

连续传递时,包与包之间的时间延迟的变化。

2.5 IP 包误差率

是错误 IP 包传送结果与成功 IP 包传送结果加错误 IP 包传送之和的比值。

3 网络流量监测方法

网络性能监测按采集流量数据的方法可以分为两种方式:

① 主动(Active)方式。它是指监测者主动发包去探测网络设备的运行情况,从网络的反馈中分析发出包的具体性能来得到需要的信息。

② 被动(Passive)方式。它是指监测者被动地采集网络中现有的标志性数据以了解网络设备的运行情况。主动方式具备实时性,不受管理权限、范围的限

制,但会对网络性能造成影响,且不准确。被动方式实时性差,但测量准确,且不会对网络性能造成影响。

下面从主动方式和被动方式两个方面来说明性能监测的方法,并列举了一些流行的监测软件。

3.1 主动方法

主动测量的方法是指主动发送数据包去探测被测量的对象,以被测对象的响应作为性能评价的结果来分析。测量者一般采用模拟现实的流量(如 Web Server 的请求、FTP 下载、DNS 反应时间等)来测量一个应用的性能或者网络的性能。由于测量点一般都靠近终端,所以这种方法能够代表从监测者的角度反映的性能。然而由于性能实际上受多种因素的影响(如流量模式,包长分布、服务类型等),所以这种测量并不准确,不一定能反映实际网络数据的性能,而且会对网络的实时性能造成影响。采用主动方法监测时可以从传输层和网络层进行。传输层的协议一般是 TCP 或 UDP。因为 TCP 是面向连接的,所以测试 TCP 的性能能够反映发送端与接收端的端与端之间的性能参数,如重传个数、建立和关闭 TCP 连接的时间、平均段大小、吞吐率等。采用这种方式的工具有 Treno ,Netperf , Iperf ,Ttcp 等。而网络层测量的对象一般是节点、链路或经过这个传输设备的包。监测的属性一般是: Delay ,Throughput ,Loss , Connectivity , Resource Utilization 等。另外,路由对性能的影响,也是网络层要监测的关键对象。网络层性能测量,是通过发送探测包来探测发送端与接收端之间路径上的性能参数。采用这种方式的工具有 Ping , Traceroute ,Pathchar ,Nettimer 等。

3.2 被动方法

被动方法的监测是在监测点采集真实的网络数据包并统计的。这种方法的监测不会对网络运行造成影响。一种方法是采集和分析由应用程序自身产生的数据。如 Web ,FTP ,Dns 都维护一个行为的日志以用来分析该应用的性能。一个标准的 API 是 Application Response Measurements。利用 ARM 的信息,很多工具都可以用来监测应用程序的性能。但是,很多应用并没有采用 ARM API 来编码。另外,还有以下方法:

(1) Sniffer。Sniffer 是局域网上的抓包技术。在共享式的网络中,信息包会广播到网络中所有主机的网络接口。Sniffer 通过把网卡设成混杂模式,使主机接收所有到达的信息包。Sniffer 技术既适合于黑客的使用,也适合于满足网络管理员分析网络性能的需要。Tcpdump 是一个强大的 Sniffer 工具。Tcpdump 可以将网络中传送的数据包的"头"完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤。

(2) SNMP MIB。它定义了一系列对象组。一些对象是网络设备必须提供的,作为强制型对象组,另一些对象只在某些设备才用到。对象本身是按层次结构定义的,因此很容易扩充。采集 SNMP MIB 中的数据,可以得到网络设备的各种统计信息。采用这种方法的工具有 MRTG 等。

(3) Net Flow。它是 Cisco 的专用协议,用来根据路由器中 IP 层的信息,了解该路由器所传输的包表头内容。CFlowd 是一个流分析工具,用来分析 Cisco 的 Net Flow 数据。分析的数据可以用来作容量规划、趋势分析、载荷分类等。

4 网络性能监测模型的提出

RTFM 是 IETF 建立的一个工作组,它提出了一个描述和测量网络流量的通用框架,根据该框架,本文在 RTFM 的基础上提出了基于 TCP/IP 的网络流量监测系统的模型,该模型分为四个模块:规则输入系统、流量采集系统、数据分析系统及数据库系统,如图 1 所示。

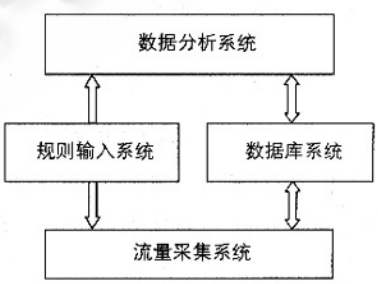

图 1　系统模型

在此模型中,流量采集系统用于测量实时网络流量,并根据规则输入系统设置的规则对网络流量进行过滤和聚类,得到有效数据,存入数据库系统中,并将之提供给数据分析系统进行处理。数据分析系统处理

有效数据，获得网络流量的变化和分布信息，从而对网络运行行为进行预测、调整和管理。

该系统模型的流程如图 2 所示。

(1) 根据设定的规则采集流量数据，放入缓冲池中。

(2) 从缓冲池中获得所需信息，进行包处理。

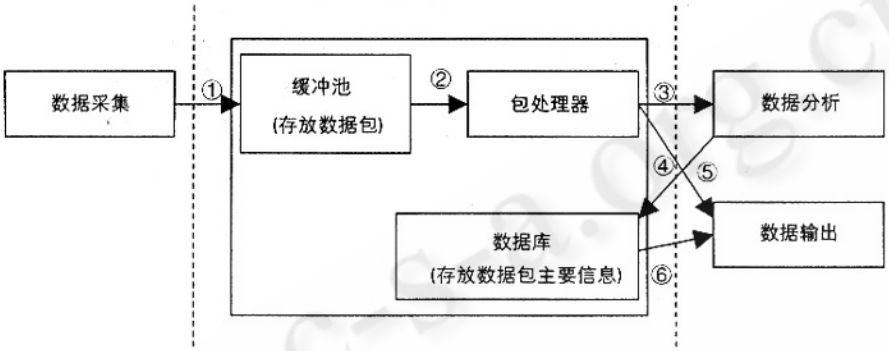

图 2　系统流程

(3) 从包头中获取进行流量分析的统计值，定时记录当前流量数据，并更新历史流量数据。

(4) 存储流量信息：包括网络流量、主机流量、协议分布、主机连接及历史流量数据等。

(5) 对网络中的实时流量进行分析，并显示流量数据(以曲线、图表等多种形式来显示)。

(6) 显示历史流量数据形式(以曲线、图表等多种形式来显示)，提供异常流量报警机制，并生成网络性能报告。

5　IP 网络性能监测的关键技术

网络流量监测技术主要涉及网络性能的测量参数的选取，测量指标的确定，具体参数的测量方法(包括测量点的布置，测量结果的采样方法等)，网络性能的评测方法，网络性能的控制与调整策略等内容。网络流量测量有 5 个要素：测量时间、测量对象、测量目的、测量位置和测量方法。下面着重对流量监测系统模型所涉及的几个关键技术进行介绍。

5.1　网络性能参数的采集方法

流量数据的采集是整个系统的基础，目前流量数据的获取一般有三种方式：基于路由器的方式、基于代理机制方式和基于监听方式。

基于路由器的方式指直接利用由器上的 MIB 库中的网络流量信息。其优点是网络结构简单，不必增加另外的硬件设备，能充分利用路由器和交换机的资源。其缺点是会定时或不定时地占用一些网络资源，增加了路由器和交换机的负载。

基于代理机制的方式是指用一台工作站跨接在网络入口处，从物理上把内部网络和外部网络隔离开。无论外界访问内部网络还是内部网络访问外界，都必须在工作站上有相应的代理进程代理其活动。这样，通过代理软件就可以统计出网络访问的源地址、目的地址、数据通信的总字节数、访问时间信息等，记入日志文件。代理机制的优点是：可以进行用户认证，方便地确认用户的访问权限，安全可靠。缺点是：它在物理上隔断了物理电路，必须经过软件过滤，这样会带来较大的时延，尤其对于高速网络的时延更为明显和难以接受，将严重地降低网络的性能。

基于监听的方式。虽然现在有许多单位的主干网络采用高速非共享介质的网络结构，如 ATM、FDDI、交换式以太网，但与外界互连的绝大部分仍是依赖于共享介质的网络，如以太网。在共享介质网络中，流经这一网络的任何数据包均可以由这一网段务器的硬件配置要求要高一些，以避免不能及时处理监听到的数据包。该方式是对所监听网络影响最小的一种，但是如何确保完整的流量数据是工作的难点的任何一台机器捕获。只要把用作网络流量分析的服务器安装在与外界互连的网段中，将该机的网卡设置成“混杂”模式，就可以捕获网络进出的所有 IP 数据包，并对 IP 包进行解析重组，就可以得到源地址、目的地址、数据量、应用协议等所需信息。其优点是：不改变原来网络结构，不增加网络负载，不占用网络资源，不涉及网络的时延，不影响用户对网络的使用。

在本文提出的系统模型中，采取了基于监听的方式。通过创建 Raw Socket，并将其属性设置为低级别操作模式（SIO_RCVALL），可以实现对所有数据包的监听，并从中获取流量数据以进行分析。利用 Raw Socket 实现 Sniffer 的方法，实现起来比较简单，但只能截获 IP 层以上的包，数据包头不含帧信息。对一些特殊的要求不能满足。从目前网络流量模型的分析可以看出，整个网络流量中主要是 TCP/IP 流量，TCP/IP 流量的变化基本反映了整个网络流量的变化，因此可以用 TCP/IP 流量代替总流量来分析网络性能，即可以用 Raw Socket 来获取流量信息。

5.2 网络性能的采样测量技术

大多数的网络流量监测技术都是对网络中的每个数据包逐个进行解包分析，并将结果插入数据库的有关表中，并以此在内存中建立网络流量矩阵。随着 GB 以太网的出现和高速网络技术的发展，网络流量模式不断变化，流量矩阵也会不断变化，这会对 CPU 的负荷产生不可预料的影响，甚至可能因此导致整个系统的崩溃，同时也会增加对内存的需求，考虑到网络负载和探测器负载，在本文提出的系统模型中，对于一些参数不采用长时间的连续测试，而是要采用适当的采样技术，即在时间轴上依据一定的算法，抽取部分测量时间点，在测量时间点上对关心的参数进行测量并记录。

在时间轴上选取采样时间点的算法很多，主要包括以下两种。

（1）传统的非自适应性采样技术。主要有周期采样（systematic sampling or periodic sampling），即简单的固定时间间隔周期性数据采样，在后处理过程中依据一定的线性预测算法进行建模，使点数据延展为连续数据；随机抽样（random sampling），即抽样间隔是通过一个函数 G（1）来随机确定。RFC2330 中推荐使用泊松抽样的方法；分层随机抽样（stratified random sampling），即将周期抽样中的固定时间间隔与随机抽样结合起来，实现在固定的时间间隔内只随机的采集一个样本。

这些传统的采术技术只适用于测量一些有预测模型或网络流量有周期性变化特性的流量，而当实际流量与预测模型不一致或并不呈现周期性变化特性时，这些方法并不十分理想。

（2）自适应采样技术，即根据已获得的样本数据动态的调整采术频率。目前有两种常用的方法：一是线性预测法（Linear Prediction – LP），另一种是模糊逻辑控制法（Fuzzy Logic Controller – FLC）。前者是通过预测下一个样本的值，来调整样本的采样间隔。而后者是模拟人脑的逻辑行为编写模糊规则，根据流量变化特性，调整样本的采样间隔。

采样算法对数据采集的效果影响很大。如果采样算法不合适，将会丢失信息，产生误差，往往不能即时准确地捕获网络中的异常事件，无法实现正常的网络管理。在本文提出的系统模型中，对 FLC 法进行了改进，通过重新定义流量变化值，来减少 FLC 法中的输入变量维数，大大的减少了模糊规则，同时通过实验验证，很好的实现了采样效果。

6 总结

随着计算机网络的普遍使用，网络范围的扩大，网络管理成为一个重要的问题，而网络流量监测网络流量监测提供了一种在实际环境中探索网络特性的手段。本文概述了目前在网络性能监测方面的发展、技术和理论，提出了一个新的网络流量监测模型，并重点介绍了流量采集系统的实现及自适应采样技术的应用，这对于网络性能的研究，尤其是高速网络性能的研究具有十分重要的意义。

参考文献

1 唐海娜等，网络性能监测技术综述，计算机应用研究，2004 年第 8 期。
2 聂荣等，关于实时网络流量测量的研究，电信科学，2004 年第 9 期。
3 杨策等，网络流量监测技术及性能分析，空军工程大学学报（自然科学版），第 4 卷第 1 期。
4 蔡伟祥等，流量采集在网络性能监测与分析系统不的改进和实现，计算机工程，第 29 卷第 15 期。
5 高琴等，一个网络流量监测系统的设计与实现，现代电子技术，2005 年第 4 期。
6 Edwin A. Hernandez 等，Adaptive Sampling for Network Management. HCS Research Lab 2000.