一种面向网络管理的接入网测度模型*)

杨 艳 丁 伟 程 光 龚 俭
(东南大学计算机科学与工程学院 南京 210096)

摘 要 网络测度是网络测量的基础,对于网络行为学的研究具有重要的意义。TCP层的测度和IP层的测度各有优劣,将这两者的优点结合起来是一项很有意义的课题。本文以IP报文传递方向为背景,分别提出了面向TCP连接和面向IP接入网的报文平衡测度。通过对TCP协议机制的分析,给出了前者取值范围的计算公式并讨论了将其映射到后者的方法,从而将这两种测度的优点结合起来。借鉴医学测度研究的方法,我们给出了后者"健康"范围的参考取值区间,并进一步讨论了测度计算的时间粒度的选取问题,使其成为一个可以实时衡量网络运行健康状况的实用指标,从而建立起一个完整的模型,可以直接应用于实际的接入网络管理。

关键词 接入网,报文平衡测度,网络管理

A Metric Model for Access Network Management

YANG Yan DING Wei CHENG Guang GONG Jian
(Dept. of Computer Science & Engineering, Southeast University, Nanjing 210096, China)

Abstract Network metric is the foundation of network measurement and plays a significant role in the research of network behavior. Both TCP layer oriented metrics and IP layer oriented metrics have advantages and disadvantages. Therefore, to take advantage of both is a meaningful subject. This paper gives quantitative balance metrics of bidirectional packets for both TCP connection and IP access network based on the direction of packet delivery. By the analysis of TCP protocol specification, the formula to calculate the former is presented and how to map the former to the latter is discussed. Then the "helth" range of the quantitative balance metric for access network is given based on real trace and by referring to the method in the research of medical metrics. as well. In addtion, the selection of time bin to calculate the metric is also discussed, thus makes it a utility index to evaluate the running state of the network. So, a complete model is established which can be applied directly to access network management.

Keywords Access network, Packet quantitative balance metric, Network management

1 引言

随着规模的急剧膨胀,互联网面临着多方面的挑战,迅速增长的流量增加了网络管理的复杂性,对网络运营管理提出了新的任务要求。要合理地解决这些问题,使网络能向用户提供更优质的服务,就要求对网络的行为特性和规律有深入的了解。而目前对Internet的特性和用户行为的把握主要是通过网络测量和流量分析进行的,流量分析主要是基于概率统计的方法。

在Internet中,TCP流量在网络流量中占绝对优势[1],90%以上的Dos攻击也是使用的TCP[2],所以TCP的流量行为主导了网络行为,成为网络行为学研究的重点。网络测量应主要着眼于TCP流量,因而在本文中,对于传输层我们主要考虑TCP。网络测量基于网络测度,这样网络用户和网络服务提供商能对网络的性能有一个统一的认识。在RFC2330中,测度被定义为"在运作的Internet中,有一些关于Internet性能和可靠性的参量,这些参量的值是我们所希望知道的,当这样一个参量被详细说明以后,这个参量就可以称之为一个测度"。

网络测度可以分为面向传输层的(尤其是TCP)和面向IP层的。大部分面向连接的测度都是基于状态的,由于需要维系所有连接的信息,所以很难实时计算,但它带有更多的语义信息,更易于分析和建模。而IP层的测度建模困难,但它是无状态的,很容易实时获取,目前在网络管理和网络安全领域的应用还比较少,但其实时获取的特性使其在实时性要求较高的场合具有无可比拟的优势。

实际上,单纯地定义这些测度并不非常困难,困难的是如何在实际中使用这些测度。这个困难体现在2个方面,一个是测度的获得过程(包括参数获取和计算2个阶段),另一个是相应测度正常范围的边界值的确定。目前,在网络管理和监测领域已经提出了部分测度。而大部分的机制,尤其是在网络安全领域来抵抗SYN攻击,比如Syn cache[4], SynDefender[5], Syn proxying[6]等,都是基于状态的,需要维系TCP连接的信息,这大大降低了端到端的TCP性能并且很难应用于大规模网络环境。

关于网络流量的平衡性方面已经有了一些研究成果。从字节(BPS)的角度来看,网络的进出流量是不平衡的[7],但从报文(PPS)的角度来看结论却有所不同。文献[8]表明在

*)本课题得到国家973重点基础研究发展规划项目基金(2003CB314804)资助。杨 艳 硕士研究生,主要研究方向为网络行为学;丁 伟 教授,博士生导师,主要研究领域为网络行为学、网络安全、网络测量;程 光 副教授,主要研究领域为网络行为学、网络安全、网络测量;龚 俭 教授,博士生导师,主要研究领域为网络管理、网络安全、网络行为学等。

TCP的控制报文之间存在一种宏观平衡性，但这种平衡性主要是着眼于TCP的控制报文。

本文的主要贡献在于从网络双向报文的平衡性出发，提出了面向连接和面向接入网的报文平衡测度并将两者关联起来，前者面向连接而后者面向IP网络。通过挖掘这两个报文平衡测度的定量关系，我们取长补短，将对前者的分析转化为对后者的计算。通过借鉴医学测度边界的设定方法，本文为后者确定了正常的参考范围，使其可以应用于实时性要求较高的场合，并讨论了时间粒度的选取问题，建立起了一个完整的测度模型。该模型可以实时地为网络管理、用户行为分析、负载平衡以及网络服务质量控制等提供依据，也可以迅速地发现网络的突发流量和异常流量，对网络管理和网络安全检测有积极的意义。

2 数据来源说明

接入网是指在Internet中一个有出口和主干网相连接的网络，在本文中指的是校园网(园区网)。这类网络没有穿透型流量，所有流量都是本网络用户的行为结果。从IP地址的角度来看，其特点是该网络分配到的是多个连续的IP地址块，其IP地址的数量为一个或多个C聚类。本文分析的数据由两个trace组成，trace1[9,10]来源于WIDE主干网的跨太平洋的100Mbps链路，收集于2005年1月7日，持续时间为24h，该trace是下文中获得TCP连接不同方向的报文比的数据来源。Trace2来源于一个高速网络测量系统WATCHER[11]，该系统运行于CERNET的一个省网边界，trace的收集时间为2005年11月10日，持续时间为24h，该trace是后面进行实例分析的主要数据，它是采用被动测量技术，在省网到地区主干的边界路由器上进行采集并存储的。所有进出省网的报文都会经过该边界，采集过程中没有采用抽样技术，所有的报文头都被完整地采集下来并存储。采用这组数据的主要原因是我们能够获得相应接入网的构成信息，这组数据中的局部经处理后已在www.njnet.edu.cn网站公布。经统计，该省网内的接入网有81个，每个接入网分配到的IP地址块都是由一个或多个连续的C类地址块构成的，每个连续的C类地址块包含大于1的整数个C聚类。

3 TCP连接中不同方向的报文比分析

考虑一次完整的TCP连接，包括3个阶段：建立连接、传送数据和断开连接。在TCP连接建立时，需要三次握手，连接发起方发送出去的报文数为2，接收到的报文数为1；在进行数据传送时，TCP使用一种被称为滑动窗口协议的流量控制方法，该协议允许发送方在停止发送并等待确认前可以连续发送多个分组，TCP协议的这种实现机制隐含了发送报文和应答报文是存在一定约束关系的；断开连接时需要四次握手，连接双方发送和接收到的报文数均为2。由上述分析可以推断，连接双方发送的报文数是存在一定比例关系的。设TCP连接的双方分别为X和Y，我们假设X和Y的发送报文比$R_{X\to Y}\in[a,b]$，对应的误差为$\%\alpha$，这时称$R_{X\to Y}\in[a,b]$在误差范围$\%\alpha$内成立。当$\%\alpha$足够小时，我们可以近似认为$R_{X\to Y}\in[a,b]$成立。

不失一般性，设在一次完整的TCP连接中，从X到Y的报文数不小于Y到X的报文数，则有$R_{X\to Y}\in[1,\lambda_1](1<\lambda_1<\infty)$，同时$R_{Y\to X}\in[\frac{1}{\lambda_1},1]$。所以在一般情况下，不管TCP连接的双方$X$和$Y$发送报文的情况如何，$X$和$Y$的发送报文比为：

$$R_{X\to Y}\in[\frac{1}{\lambda_1},\lambda_1] \tag{1}$$

为了得到一次TCP连接中连接双方发送报文的比例关系，我们对trace1的报文按TCP连接进行统计。设连接的双方中发送报文数较多的一方为A，发送报文数较少的一方为B，设A方发送的报文数与B方发送的报文数之比为$R_{A\to B}$，显然$R_{A\to B}\subseteq[1,\infty)$。考虑到一个正常的TCP连接至少需要6个报文，所以在这里我们只选取交互报文数在6个以上的TCP连接。在这次实验中，我们从一个连续的时间段中按上述正常TCP连接的定义，选择了连续的100万个连接。图1给出了$R_{A\to B}$在不同区间范围内的连接数占总连接数的百分比。其中，$R_{A\to B}$在区间[1,2]之间的TCP连接的个数为951607，占TCP连接总数的95.2%；$R_{A\to B}$在区间[1,2.5]之间的TCP连接的个数为981435，占TCP连接总数的98.14%。

若取$\lambda_1=2$，则(1)式中$R_{X\to Y}\in[\frac{1}{2},2]$，$\%\alpha=4.8\%$；取$\lambda_1=2.5$，则$R_{X\to Y}\in[0.4,2.5]$，$\%\alpha=1.8\%$。在下文的分析中，我们取5%为可以接受的误差范围，这样我们有：

$$R_{X\to Y}\in[\frac{1}{2},2] \tag{2}$$

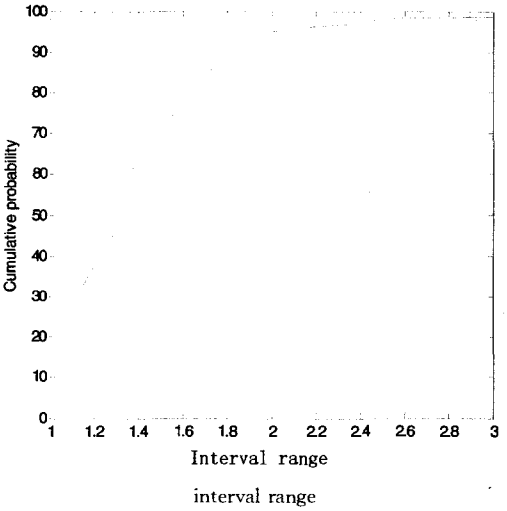

图1 $R_{A\to B}$在不同区间的百分比

4 报文平衡测度的定义和性质

定义1 设在一个给定的时间段t内，某接入网接收到的报文数为$\lambda_{in}(t)$，发送出去的报文数为$\lambda_{out}(t)$，称函数$x(t)=\frac{\lambda_{in}(t)}{\lambda_{out}(t)}$为$t$时间段内该接入网的进出报文比。

定义2 设li为接入网和外网的一次TCP连接，$\lambda_{in}(li)$为该接入网接收到的对应该连接的报文数，$\lambda_{out}(li)$为该接入网发送出去的对应该连接的报文数，则称函数$R(li)=\frac{\lambda_{in}(li)}{\lambda_{out}(li)}$为连接$li$的进出报文比。

函数$x(t)$和$R(li)$可以认为是测度，前者可以基于接入网的边界网络设备通过SNMP比较容易地实时获取。而后者$R(li)$虽然根据上一小节的分析存在一个稳定的边界，但具体测度值的获取则因为需要将报文组成TCP流，因此很难实时完成。在下面的讨论中，我们将围绕这两个测度之间的联系进行，希望能够获得它们之间的定量的关系，并由此展开

进一步的研究。

定义 3 设在一个给定的时间段 t 内，某接入网接收到的报文数为 $\lambda_{in}(t)$，发送出去的报文数为 $\lambda_{out}(t)$，则称函数 $d(t)=\frac{\lambda_{in}(t)-\lambda_{out}(t)}{\lambda_{in}(t)+\lambda_{out}(t)}$ 为 t 时间段内该接入网的报文平衡测度。

显然，$d(t)=\frac{x(t)-1}{x(t)+1}$。

定义 4 设 li 为接入网和外网的一次 TCP 连接，$\lambda_{in}(li)$ 为该接入网接收到的对应该连接的报文数，$\lambda_{out}(li)$ 为该接入网发送出去的对应该连接的报文数，则称函数 $D(li)=\frac{\lambda_{in}(li)-\lambda_{out}(li)}{\lambda_{in}(li)+\lambda_{out}(li)}$ 为该连接 li 的报文平衡测度。

定理 1 设单个 TCP 连接的报文比 $R_{X\to Y}$ 在区间 $[a,b]$ 之内，在 t 充分大并只考虑 TCP 流量的情况下，$d(t)$ 的取值区间为 $[\frac{a-1}{a+1},\frac{b-1}{b+1}]$。

证明：在上文中对 TCP 连接的收发报文比进行了分析，设单个 TCP 连接的报文比 $R_{X\to Y}$ 在区间 $[a,b]$ 之内，所以对该接入网与外网建立的某个 TCP 连接 li 而言，$a\leqslant R(li)=\frac{\lambda_{in}(li)}{\lambda_{out}(li)}\leqslant b\Rightarrow a\lambda_{out}(li)\leqslant\lambda_{in}(li)\leqslant b\lambda_{out}(li)$。而 $d(t)=\frac{x(t)-1}{x(t)+1}$ 是关于报文进出比 $x(t)$ 的增函数；$x(t)>1\Leftrightarrow d(t)>0$，$x(t)\leqslant 1\Leftrightarrow d(t)\leqslant 0$。

在只考虑 TCP 流量的情况下，接入网所有的流量是由多个 TCP 连接构成的。当 t 充分大时，可视为每个连接都是完整的，设 t 时间内的连接数为 n，则有 $\lambda_{in}(t)=\sum_{i=1}^{n}\lambda_{in}(li)$，$\lambda_{out}(t)=\sum_{i=1}^{n}\lambda_{out}(li)$

又 $\because a\lambda_{out}(li)\leqslant\lambda_{in}(li)\leqslant b\lambda_{out}(li)$，$\therefore\sum_{i=1}^{n}a\lambda_{out}(li)\leqslant\sum_{i=1}^{n}\lambda_{in}(li)=\lambda_{in}(t)\leqslant\sum_{i=1}^{n}b\lambda_{out}(li)$，故由 $x(t)=\frac{\lambda_{in}(t)}{\lambda_{out}(t)}=\frac{\sum_{i=1}^{n}\lambda_{in}(li)}{\sum_{i=1}^{n}\lambda_{out}(li)}$，$\Rightarrow a\leqslant x(t)\leqslant b$，因为 $d(t)$ 关于 $x(t)$ 的增函数，所以 $d(t)$ 的取值区间为 $[\frac{a-1}{a+1},\frac{b-1}{b+1}]$。

基于第 3 小节(2)式的讨论，取 $a=1/2$，$b=2$，对应的误差范围在 5%内，则 t 时间段内接入网的报文平衡测度 $d(t)\in[-\frac{1}{3},\frac{1}{3}]$。而在网络的实际流量中，还存在一小部分的 UDP 流量，这部分流量虽然影响不大，但是可以考虑用一个大于 1 的系数来修正它带来的影响。由于 TCP 在总流量中占到 95%以上，因此这个系数可以取为 $\frac{1}{0.95}$，从而将 $d(t)$ 可能的取值范围扩大为 $[-0.35,0.35]$。

$d(t)$ 的取值区间的上下界可以视为网络平衡性的一条警戒线("红线")。考察 $d(t)$ 的值，可以对网络进出报文的情况有一个定性的认识：(1) $d(t)=0$ 表示该段时间内网络的进出报文数相当；(2) $d(t)\in(0,0.35]$ 表示该段时间内进入网络的报文数要多于从该网络出去的报文数，且 $d(t)$ 的值与右端点值越接近，两者相差越大；(3) $d(t)\in[-0.35,0)$ 表示该段时间内从该网络出去的报文数多于进入该网络的报文数，且和左端点越接近，两者相差越大；(4) 当 $d(t)\notin[-0.35,0.35]$，即 $d(t)$ 的值落在该区间之外，这表示该段时间内接入网报文的进出情况存在异常，这种异常可能是因为一个时间段内有大量突发的 UDP 流，也有可能是链路出了故障等，甚至网络的安全性受到了威胁(比如外部对于内网的 DDos 攻击会导致进入网络的报文数急剧增加，此时 $d(t)$ 的值可能就会落在该区间范围之外)，所以对于网络进出报文平衡测度的统计分析可以为网络管理员更高效地进行网络管理、理解用户行为、诊断安全攻击提供一些启示性的信息，从而有利于尽早地采取措施来解决网络问题或者优化网络性能。从这个意义上而言，报文平衡测度可以视为衡量网络结构、用户行为和运行状况的参考指标之一。

上面的分析是基于 t 值为"充分大"这样一个条件的，在实际操作中这个"充分大"实际上是一个时间粒度问题，这个问题将在下面的第 6 小节中进行分析。

对单个接入网络而言，报文平衡测度从一定程度上反映了网络的状况以及用户的行为，如网络内部有大量的服务器存在而导致出去的报文数明显多于进入的报文数(反映了特殊的内部网络架构，此时 $x(t)<1$，$d(t)<0$)，或者有大量的用户下载资源而导致进入的报文数明显多于出去的报文数(反映了用户的行为，此时 $x(t)>1$，$d(t)>0$)。基于这个简单的事实，我们对 trace2(省网到地区主干一天的报文)进行了面向这两个测度的分析，从中可以大致看出，虽然不同时间段内报文进出的绝对数量可能变化很大，但大部分接入网进出报文数的比例关系波动并不是很厉害。

5 报文平衡测度指导下的网络健康状况评估方法

5.1 评估方法

网络的运行状况是否正常(健康)，是可以通过一系列测度来反映的，如单向延迟、丢包率等。而医学上对于健康的定义也是通过一系列测度来衡量的，如血压、血糖、心率等。如何用某种测度来评估健康状况，医学上的处理方法可以为我们提供借鉴。在医学研究中，在未知分布的情况下，常对一组同质个体作某项指标的测定，以确定该指标的参考范围(以往称之为正常值范围)[12]。在未知报文平衡测度的分布规律的情况下，我们也可以根据医学统计原理中的一些思想和方法来确定接入网报文平衡测度的参考范围。为此我们先参考医学研究的方法，给出一个关于百分位数的定义。

定义 5 设 $(D_1,D_2,\cdots,D_n)$ 为取自总体 X 的一个样本，$(d_1,d_2,\cdots,d_n)$ 为样本的观察值，将这些值按大小递增顺序排列成 $d_1\leqslant d_2\leqslant\cdots\leqslant d_n$)。设 y 为一个数，满足条件：理论上有 i%的观察值不比它大，有 $(100-i)$%的观察值不比它小，则定义 y 为该组观察值的 i 百分位数。

根据医学的方法，绝大多数正常的测定值都应在参考范围内，这个"绝大多数"习惯上指 80%，90%，95%和 99%。如何选取合适的百分界限是确定参考范围的关键之一。若要减少误报率，则要选取较高的百分界限；若要减少漏报率，则应选取较低的百分界限。在实际情况中可以根据具体应用需求确定。在未知分布的情况下，取 α 百分位数和 β 百分位数分别为参考值范围的上下界值，由此来确定参考范围的区间。用 $d(t)$ 值来衡量进出网络的报文的平衡性，这时大约有 $(1+\alpha\%-\beta\%)\times 100\%$ 的网络，其报文平衡测度值落在该参考范围区间外。在医学上，通常的做法是取 $\alpha=2.5$ 和 $\beta=97.5$。在这里可以根据网络的实际情况(主要是期望的误报率和漏报率)来确定 α 和 β 的值。如果从报文平衡性这个测度来衡量网络的健康运行状况，那么报文平衡测度值落入该参考范围内的这些网络，其运行可以认为是近似健康的，否则预示着存在潜在的问题或者特殊性，需要进行特别的关注或者适当

的调整。我们将以上述的定义和方法为基础，基于 trace2，给出 $d(t)$ 的一个“健康”的参考范围，并将这个参考范围视为基于该测度的另一条警戒线（“黄线”）。

5.2 数据分析

根据上面的介绍，trace2 的数据来源于 81 个接入网。我们取其中 8h(12:00～20:00)的数据，并以 4h 为时间粒度进行分析，以满足充分长时间这一条件。这样获得的样本观测值的数量为 $81\times2=162$ 个。保留平衡测度值在[－0.35，0.35]之间的样本个体，再将所得到的各个 d 值进行分组和频数统计(取分组组数为 14，组距为 0.05)，其频数分布图如图 2 所示。

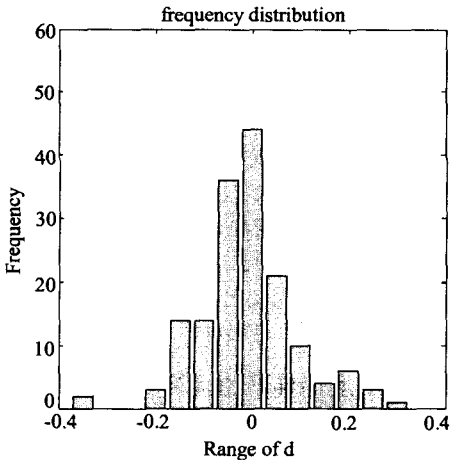

图 2 测度 d 的频数分布图

可以求出报文平衡测度均值 $\bar{\eta}=0.014$，报文平衡测度的标准差 $S=0.061$。由图 2 可以看出该频数分布基本以均数 0.014 为中心，左右两侧接近对称，靠近均数的两侧频数较多，离均数愈远频数愈少，左右两侧相对分散，形成一个中间区域频数比较集中、两侧频数逐渐减少接近对称的分布(我们用常规方法进行了检验，并不能证明其服从正态分布)。

根据前述的定义和方法，在未知分布的情况下，取 $\alpha=2.5$，$\beta=97.5$，即 2.5 百分位数和 97.5 百分位数分别为参考值范围的上下界值，得到进出报文平衡性的参考范围[－0.189，0.236]。显然，这个区间小于上小节分析得出的[－0.35，0.35]范围，因此我们将这个区间([－0.189，0.236])定义为该测度的“绿色”范围，表示完全“健康”；将[－0.35，－0.189]和[0.236，0.35]两个区间定义为该测度的“黄色”范围，表示需要“警惕”；而将小于－0.35 和大于 0.35 的取值定义为“红色”范围，表示出现问题。从而可以更形象地将[－0.189，0.236]和[－0.35，0.35]两个区间的边界分别称为“黄色警戒”线和“红色警戒”线。

6 时间粒度分析

以上所有的分析均是在“时间充分长”这样一个条件下进行的，而 4h 这样的时间对该测度的实用性而言是不能接受的。那么对一个稳定运行的接入网而言，选取怎样的时间粒度来计算报文平衡测度以评估网络状况是合适的呢？本节我们选择了一个接入网基于统计的方法，对该问题进行了简单的分析。该方法的思路来源于文献[13]，在这篇文献中得出了 TCP 流的超时时间为 64s 这个被广泛引用的结论。

图 3 是根据 00:00～09:00 时间段内该接入网以 300s 为时间粒度的进出报文数。从这 9h 的实际流量可以看出，在不同的时间段进出报文的绝对数量变化较大，但大部分时间内发送的报文数和接收到的报文数却相当接近。

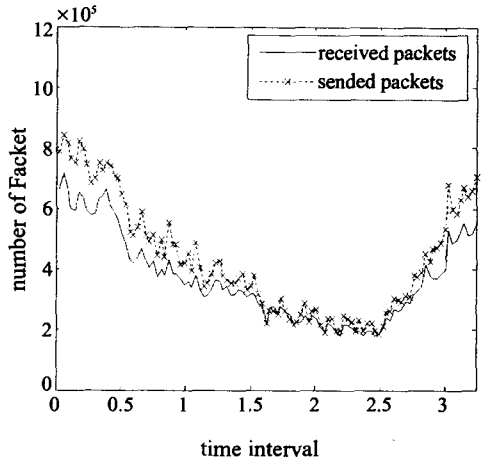

图 3 00:00～09:00 以 300s 为时间粒度进出的报文数

图 4 和图 5 是在 00:00～09:00 时间段内，分别以 600s 和 300s 为时间粒度，计算的该接入网各个时间粒度内对应的报文平衡测度的值。可以看到，这两个不同的时间粒度对应的报文平衡测度曲线的大致趋势是一致的，说明这两个时间粒度的选取并没有本质的区别，而当时间粒度取为 60s 时(如图 6 所示)，在某些点出现了明显的差别，因此我们认为将时间粒度取为 300s 也就是 5 分钟是合适的。

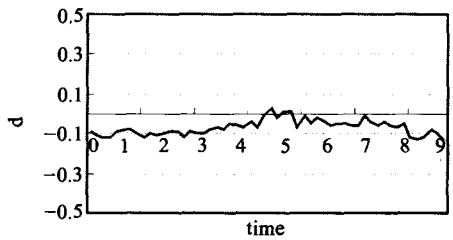

图 4 以 600s 为时间粒度计算的进出网络报文平衡性指标 $d(t)$ 的变化

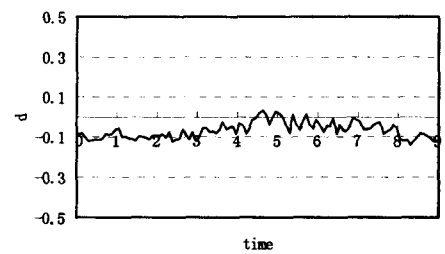

图 5 以 300s 为时间粒度计算的进出网络报文平衡性指标 $d(t)$ 的变化

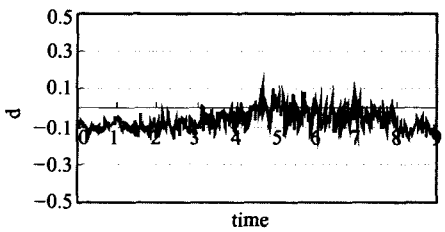

图 6 以 60s 为时间粒度计算的进出网络报文平衡性指标 $d(t)$ 的变化

7 对模型其他相关问题的考虑和实验验证

本文以上各小节的讨论均在一个相对理想的条件中完成，在实际环境中，可能还需要考虑以下这些因素：

· 对于一个特定的接入网而言，当 d 的值长时间稳定在一个范围内，这是它网络架构稳定的一个体现。d 的值从一个侧面反映了该网络内服务器和用户行为的相互关系，这是一些相对稳定的因素。当 d 的值偏离平衡性的参考范围，这时进和出的报文数相差过大，如果进出的路由是不一致的，这时可能需要对路由进行动态调整，以实现负载均衡。

· 对某些网络而言，进出网络的流量的优先级可能是不一样的。当流量到达高峰期而因为带宽、缓存和 CPU 处理能力有限的原因不得不丢包时，根据 d 所表现的报文进出平衡性以及事先约定的服务质量等级，可以选择性地丢弃某个方向低优先级的报文。

· 接入网的规模问题。如果接入网的规模太大，少量节点的流量异常会被掩盖掉，无法引发较大差异的出现，所以上述模型要用于异常检测，对于小型或者中小型的网络规模是合适的，如校园网或者更小一点的接入网。

· 当 d 的值出现较大幅度的波动时，表示网络出现了某些异常，使得进出报文数已经趋于不平衡的状态，这时可以对网络的流量分布进行更细致的监测，突发流量的出现是可能的，需要采用合理的主动队列管理技术，另外的可能性是受到了安全攻击，需要更为有效的安全检测模块。

我们对 2004 年 4 月 17 日采集的 trace 进行了实验，该 trace 的采集点和 trace2 一样，也是来源于省网到地区主干的边界路由器。我们选取了该日 4:00～12:00 之间的数据，以上述的 5min 为时间粒度对接入网的报文平衡测度 $d(t)$ 进行计算，结果见图 7 所示。

可以看到，该测度在大部分时间内都维持在一个相对平稳的值附近，但在 8:00～9:00 之间出现了较大的波动。经过分析，这段时间的异常可能是 DDoS 攻击。

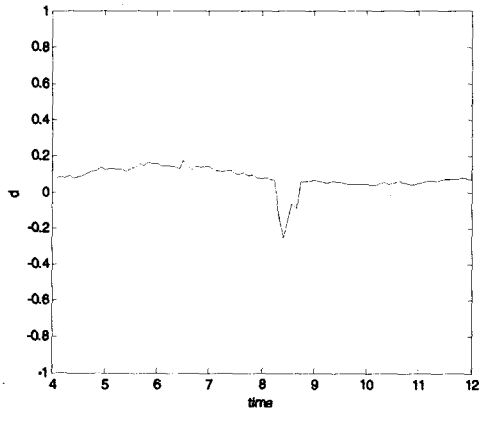

图 7 以 5min 为时间粒度计算的 4:00～12:00 之间报文平衡测度 $d(t)$ 的变化

结束语 定义合理有效的测度，是 Internet 测量标准化的要求，也是网络行为学研究的基础。实际上，定义这些测度并不非常困难，困难的是如何在实际中使用这些测度。这个困难体现在 2 个方面，一个是测度的获得过程(包括参数获取和计算 2 个阶段)，另一个是相应测度正常范围的边界值的确定。本文以报文平衡测度为切入点，具体研究了这个问题。我们从接入网和 TCP 连接两个角度分别给出了这个测度的定义 $d(t)$ 和 $D(li)$，前者是一个基于 IP 层的测度，而后者是属于 TCP 层的。根据互联网运行的基本原理，基于 IP 层的测度由于其相关的参数可以通过路由器或信道采集直接获取，因此相应测度的计算代价比较小。而面向 TCP 的测度，由于需要维护“流”信息，所花费的代价则要大很多。但 TCP 测度通常能够带有更多的语义，更有利于分析。本文所讨论的测度同样具有这个特点，$d(t)$ 的获取要比 $D(li)$ 容易许多。文中，我们基于 TCP 连接的特点对相应测度 $D(li)$ 的取值范围进行了分析，随后讨论了将这个分析的结果映射到 IP 层的 $d(t)$ 的过程和方法，并基于实际的 trace 数据和统计结果，给出了 $d(t)$(基于接入网的报文平衡测度)的一个参考取值范围[−0.35,0.35]。然后进一步基于医学统计学的方法对其进行了修正，得到了[−0.189,0.236]这个更严格的边界，并由此形成了该测度“健康”范围的“红线”和“黄线”，从而使该测度能够走向“实用”。

本文所进行的研究的意义，更重要的是测度边界的获得过程和方法，而不是具体的数值本身。一方面，这个边界数值，尤其是其中的“黄线”可以根据网络运行的情况具体调整；另一方面，我们希望这样的方法能够作用于更多的类似的测度研究中。这也是我们今后研究工作的重点之一。

参 考 文 献

[1] Fomenkov M, Keys K, Moore D, et al. Longitudinal study of Internet traffic in 1998-2003 //Winter International Symposium on Information and Communication Technologies (WISICT). Cancun, 2004

[2] Moore D, Voelker G, Savage S. Inferring Internet Denial of Service Activity//Proceedings of USENIX Security Symposium' 2001. August 2001

[3] Paxson V. RFC 2330- Framework for IP Performance Metrics, May 1998

[4] Lemon J. Resisting SYN Flooding Dos Attacks with a SYN Cache// Proceedings of USENIX BSDCon'2002. Februrary 2002

[5] Check Point Software Technologies Ltd. SynDefender. http://www.checkpoint.com/products/firewall-1

[6] Netscreen 100 Firewall Appliance. http://www.netscreen.com/

[7] 戴宣，丁伟，程光. TCP 数据流的非对称性分析. 计算机工程(已录用)

[8] 龚俭，彭艳兵，等. TCP 流的宏观平衡性. 计算机学报，2006，29(9)：1561-1571

[9] http://tracer.csl.sony.co.jp/mawi/samplepoint-B/20050107/

[10] ftp://tracer.csl.sony.co.jp/pub/mawi/tools/tcpd-tools.tar.gz

[11] 程光，丁伟，龚俭. 高速网络流量通用测量平台-WATCHER[J]//CSIT 2004 会议论文集. 南京，2004：122-128

[12] 刘筱娴. 医学统计学. 北京：科学出版社，2001

[13] claffy K C. Internet Traffic Characterization. Ph D dissertation. San Diego : University of California, 1994