ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.10, October 2006, pp.2141−2151
DOI: 10.1360/jos172141

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

高速网络中基于流速测度的动态超时策略*

周明中[1,2,3+], 龚 俭[1,2,3], 丁 伟[1,2,3]

[1](东南大学 计算机科学与工程学院,江苏 南京 210096)

[2](江苏省计算机网络技术重点实验室,江苏 南京 210096)

[3](江苏省网络与信息安全重点实验室,江苏 南京 210096)

High-Speed Network Flows' Dynamical Timeout Strategy Based on Flow Rate Metrics

ZHOU Ming-Zhong[1,2,3+], GONG Jian[1,2,3], DING Wei[1,2,3]

[1](Department of Computer Science, Southeast University, Nanjing 210096, China)

[2](Jiangsu Province Key Laboratory of Computer Network Technology, Nanjing 210096, China)

[3](Jiangsu Province Key Laboratory of Network and Information Security, Nanjing 210096, China)

+ Corresponding author: Phn: +86-25-83794000 ext 206, Fax: +86-25-83614842, E-mail: mzzhou@njnet.edu.cn, http://www.seu.edu.cn

Zhou MZ, Gong J, Ding W. High-Speed network flows' dynamical timeout strategy based on flow rate metrics. *Journal of Software*, 2006,17(10):2141−2151. http://www.jos.org.cn/1000-9825/17/2141.htm

Abstract: The measurements based on flow characteristics have been playing more and more important roles in the analysis of Network Behavior. As a main method of flow recognition, the timeout strategies have a very important impact on the correctness and performance of flow measurement. This paper firstly discusses the state-of-art of flow timeout strategies, and points out where they are applicable and their shortcomings. To deal with the short flows that take a large part of the total flows in the networks, the paper presentes a Dynamical Timeout Strategy (DToS) based on the analysis of flows' length distribution and flows' rate metrics in detail. This method could improve the performances of network measurement and the efficiency of the resource usage in measurement systems by using different timeout strategies dealing with flows that have different rate features based on analyzing the usage of target network. It could also apperceive network abnormal behavior efficiently, and trigger emergent methods to ensure the safety of measurement system. After that the feasibility and robustness of this method are analyzed. At last, some experiments are employed to show the rationality of DToS strategy. The fitness area of strategy is also anatomized in the paper.

Key words: high-speed network; network flow; flow rate characteristics; dynamical timeout strategy (DToS)

摘 要: 基于流特性的测量在网络行为分析中发挥着越来越重要的作用.超时策略作为流识别的主要标志之

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.2003CB314804 (国家重点基础研究发展规划(973)); the National High-Tech Research and Development Plan of China under Grant No.2005AA103011-1 (国家高技术研究发展计划(863)); the Key Project of Chinese Ministry of Education under Grant No.105084 (国家教育部科学技术重点研究项目); the Jiangsu Province Key Laboratory of Network and Information Security under Grant No.BM2003201 (江苏省网络与信息安全重点实验室)

Received 2005-10-08; Accepted 2006-05-16

一,对流特性测量的正确性和性能具有重要的影响.通过对现有流超时策略进行比较和分析,指出这些超时策略的适用范围和存在的问题.在详细分析网络中流长分布和速度测度各项指标的基础上,针对短流占总体流量很大比例的特点,提出了一种动态超时策略(dynamical timeout strategy,简称 DToS).该策略通过实时综合分析网络使用状况,针对不同特性的流采用不同的超时方式,从而增加网络测量性能,提高测量系统的资源利用率;并可以有效地感知可能存在的网络异常,启动应急措施,保证测量系统的安全;然后通过理论分析的方法验证该策略的可行性和鲁棒性;最后通过实验论证该超时策略在实际测量中的性能,并进一步分析其适用范围.

关键词: 高速网络;网络数据流;流速特性;动态超时策略(DToS)
中图法分类号: TP393 文献标识码: A

Internet 的发展及其用户的增加,使得各种网络服务层出不穷,导致网络流量不断增大,网络行为也变得越来越复杂.对网络行为进行分析,找出其中宏观和微观变化规律并根据掌握的情况采取相应措施,在现有软硬件的基础上提高网络服务的质量显得十分重要.传统上对网络流量的测量集中在报文层次,但是,由于网络流量的增长速度要高于计算机软、硬件的发展速度,而且报文层次的测量相对平等地分析每个报文,不能反映报文间存在的内在联系及更高层次信息,所以,单纯地基于报文层次的网络测量已不能满足网络行为观测及相关网络优化和管理的需求.

基于流的网络行为研究弥补了局限于报文层次研究的不足.所谓流,是指符合特定的流规范(specification)和超时(timeout)约束的一系列数据报文的集合[1].基于流行为研究通过分析属于特定流的一系列报文综合特性,可以在更高层次上分析网络行为,更好地为网络应用提供信息支持;可以根据具体需求采用不同流规范和超时策略得到不同流的集合,通过对数据流的分析和整形(profiling),提高网络性能和网络服务质量.目前使用频度较高的流规范主要有五元组、目的地址或者 ODflow 等[1−3],其中,五元组流规范被广泛地采用[1,4−6];超时约束将超过一定时间不活动的流定义为已终结,这样既可以对流进行进一步分析,也可以使测量系统的资源得到充分利用,超时策略的设定对流测量的精度和测量系统资源的有效使用具有较大影响.

网络流速测度是指单位时间内属于特定流的报文到达数量.流主要包含的测度有:流速测度、流长测度、流到达率测度等.从不同网络不同时段采集的数据表明[4,5,7−9],流长分布基本服从重尾分布特性,在正常情况下一般不会发生较大改变.但是,流速测度和流到达率测度会随着网络负载变化而产生波动,不同的超时方式对流识别精度产生较大影响,同时也对流识别系统的资源提出了不同的需求.

本文主要研究在五元组流规范下,采用现有不同超时策略对流测量精度和测量系统负载的影响.在分析网络实际状况,特别是网络流速特性的基础上,提出一种基于网络流速测度的动态超时策略(dynamical timeout strategy,简称 DToS).通过对不同特性的流采用不同的超时方式,增加网络测量性能,提高测量系统的资源利用率;可以有效地感知可能存在的网络异常,启动应急措施,保证测量系统的鲁棒性.

本文第 1 节详细分析现有流超时策略,指出它们的适用范围和存在的不足.第 2 节定义网络流速测度的概念,分析阐述高速网络中流速测度特性.在此基础上,本文第 3 节提出高速网络中基于流速测度的动态超时策略,从理论上分析该策略的性能、误差及其适用范围.本文第 4 节给出相关实验结果,比较不同超时策略在实际测量中的性能和误差,论证 DToS 的执行效率和可行性.最后,探讨该策略的未来进一步工作方向.

1 现有流超时策略分析

超时是流识别的重要标志之一,不同的超时对流的测量结果和资源的消耗有很大影响.如果超时设置得过长,将导致大量已经结束的流占用存储空间时间过长,大量消耗计算资源,从而导致相关的观测或调度系统负荷过重;如果超时设置过短,可能导致长流被截断(shortening)成为若干短流,使得流不断地消亡和产生,表现为系统的颠簸(thrashing)[1,4,5].所以,目前超时研究的主要方向是具体研究网络中数据流的观测特性,寻找性能和消耗的最佳平衡.

Claffy[4,5]提出了采用固定超时实现的方法,并通过实验证明其取得了比较好的效果,这些实验结果得到广

泛认可,被大量引用.但是,(1) 固定的超时不能很好地区分不同速率的流,可能会长时间保存已经结束的流,导致过多地占用存储资源;(2) 过短的固定超时可能导致流被截断,从而导致流的频繁产生和终止;过长的固定超时可能导致结束的流驻留存储空间太长,只能在其中寻找一种相对的平衡;(3) Claffy 提出并论证 64s 的超时标准在大部分正常情况下可以取得较好的效果,但是当网络出现流量异常时,固定的超时策略可能导致测试结果产生偏差甚至错误.

Rye,Cheney 等人在文献[1]中提出的 MBET 策略是针对每个流都维护一个独立的超时,并根据此流的数据包到来时间间隔、吞吐量等观测特性动态改变超时的大小,以适应流的变化.该策略在新流创建时为其设定一个足够大的超时,然后在每个超时时间到达时定期观测流吞吐量,使超时值维持不变或以 2 的指数形式递减,从而在尽可能保证流不产生颠簸和截断的同时,使消耗的存储空间最小化(使已结束的流尽快从内存中清除).但该策略也存在一些固有的问题:(1) 没有充分利用测量对象本身所具有的特点,而采用单一的时间判断机制;(2) 参数的选择影响其测量精度,设置不合理的参数可能导致测量结果和实际情况产生很大的差异.

Wang,Li 等人在文献[6]中提出了一种可能性保证的适应超时策略(PGAT),对不同应用类型的流分析其速度规律,然后通过流产生比例和流完整率等一系列测度值来精细控制流的超时.该文献给出的策略需要对流的类型作分析和判断,主要适用于长流观测,但是对短流并没有作相关优化,而且策略实现比较复杂,在文献中并没有对该策略在所需的时间复杂度上作深入分析.

Hohn,Veitch[7]提出了利用不同的超时,如协议(如 TCP 的 FIN 包)和内存控制(为新流准备空间而结束存在一定时间的流)等定义流的方式,但并没有对此作进一步的分析.这些超时策略,特别是内存控制策略,一般需要和具体的网络测量需求相结合,在必要时为保证测量性能必须牺牲其正确性.

文献[1,4,5]中的测量数据表明:在不同网络中均存在大量的短流,针对 CERNET 主干网的观测也证明了这一点.通过对不同时段流分布进行分析,短流的个数占网络流总量的 40%以上.这些短流对流总体分布和流特性有极其重要的影响,同时也在流识别过程中占用了大量系统资源.现有的超时策略都没有对此作优化处理,导致这些短流与其他流一样平等地占用系统资源.在 MBET 策略中,由于没有后续数据包的到来,短流的超时将维持策略所设置的初值,比一般流更多地占用系统资源.当网络出现流量异常时(如遭遇 DDoS 攻击或蠕虫爆发等),短流在流总量中所占比例将急剧上升,其所消耗的资源也将相应增加.因此,如果不对这一部分短流做优化处理,可能导致系统资源耗尽,从而使测试结果产生偏差甚至错误.

各种超时策略研究的主要出发点均在于协调正确地描述流分布和资源利用之间的冲突,寻找两者之间的平衡点,在保证一定正确性的条件下尽可能地减少所需系统资源.现有流分类和识别方法一般使用单一的超时判断机制[1,4,5,7],在判断精度和性能上各有千秋,但均不能最大限度地达到两者之间的最佳平衡.因此有必要继续改进流超时的判定方法,结合各种流判断机制的优点,扬长避短,在保证流的识别精度的条件下更合理地使用系统资源.

2 高速网络中流速测度特性分析

流速测度是描述网络中属于特定流的报文到达速率的一个指标,具体表现为:在指定的测量点(一般为边界路由或者主干节点),单位时间内到达的属于特定流的报文的数量.由于每个测量点单位时间内会同时存在若干活跃流(指有报文到达的流),而每个活跃流的流速也不尽相同,所以,基于测量点的流速测度不仅反映当前网络流量状况,同时也刻画了网络中流的平均速率分布状况.本文主要从几个方面来考察特定网络流速率测度:随机流内报文到达速率、特定流平均报文达到速率、流速平稳性等.为便于表达,本文将平均流速较快的流称为快流,反之称为慢流.

2.1 流速测度特征分析

文献[4,5,7,9]对网络中流长重尾分布作了比较详细的分析,对 CERNET 主干华东北地区节点长期监测数据也验证了这一点.所谓流长重尾分布是指占流总数绝大部分的是短流而占极小部分的长流却承载了网络的大部分负载.对网络实际负载影响较大的是极小部分的长流,而短流由于其所占比例极大,它们对路由等网络设备

和网络应用前端测量系统的性能有较大影响.因此,本文首先将流按照流长分为长流和短流两种类型(短流定义为流长<6 个报文的流,其他流定义为长流),然后按照流的不同类型对网络中属于该流的流速测度进行分析.采用流长6个报文作为流长类型分界的主要依据在于:(1) 该部分流在网络中大概比例在90%以上,也就是说占据了网络中流的主体;(2) 由于在 Internet 中 TCP 流所占比例在 97%以上[2,3,9],而一个正常的 TCP 连接至少需要 6 个报文(除非特别说明,本文涉及的流都是双向流)[10],也就是说,只有报文数大于 6 个的 TCP 流才有可能建立有效的 TCP 连接,所以在保证识别精度的前提下,尽早发现并终结那些无效 TCP 连接对提高测量系统的性能显得尤为重要.

图 1 描述了随机流内报文到达时间间隔和特定流平均报文到达时间间隔分布曲线.数据来自于 CERNET 主干华东北节点某日不同的时段,前者采用抽样的方式截取来自不同流的报文到达间隔,后者采用流抽样的方式截取若干条完整的流的报文到达间隔,然后计算平均值.由分布曲线可以看出:两者都基本服从重尾分布的特征,图 1 中左图说明绝大部分报文到达间隔很小,只有一小部分报文间隔比较大;右图说明大部分流的平均速率较大,它们的平均报文到达间隔要远小于 1s(超过 50%的长流平均到达报文间隔小于 0.37s),但是其中存在一部分平均报文到达间隔很大的慢流,使得所有流平均报文到达时间间隔的均值为 1.88s.因此从总体来看,速率较大的流占流总数的绝大部分,而极少量速率很小的流对网络中流平均速率产生较大影响.

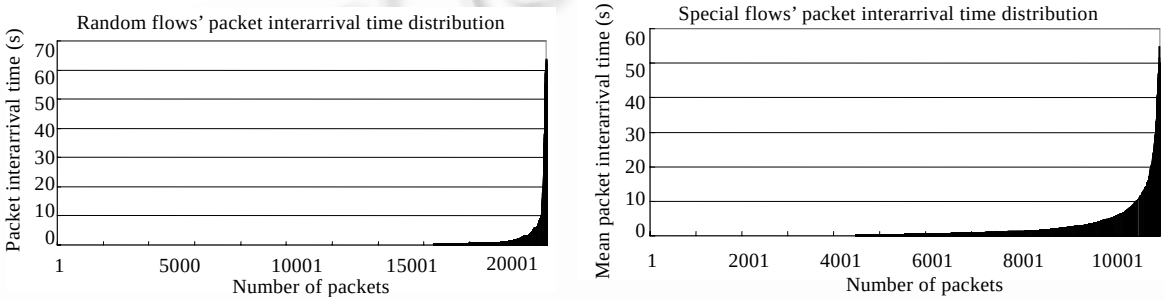

Fig.1 Distributions of random packets interarrival time and special packets interarrival time

图 1 随机流内报文到达时间间隔分布和特定流平均流内报文到达时间间隔分布

在流速率分析的基础上,本文基于流内报文到达时间的方差对流速率平稳性进行了分析.报文到达时间的方差在一定程度上可以表现出同一个流中报文到达时间的平稳性.一般来说,方差越大,说明报文到达时间越不平稳,但是如果均值本身比较小,即使方差较小也不能说明该流的报文到达时间变化不剧烈,因为方差只是用来表明序列取值分散程度的一个指标,而不是用来衡量序列取值偏离均值程度的指标.因此,在描述流速测度的流速平稳性之前,本文引入偏差系数的概念.

定义 **1**. 将序列的每个值除以序列均值作为新的序列,然后计算该序列的方差,该值称为原序列的偏差系数.

偏差系数描述了序列取值偏离均值的程度,所以可以用来描述流内报文到达速率的平稳性.图 2 对随机采集自 CERNET 的 2 065 个不同长度流的流内报文到达时间进行考察,主要对象有 3 个:流内报文到达时间均值、方差和偏差系数.值得注意的是:由于流是按照一定比例随机选取的,反映了流的实际分布状况,所以在流长较短处对应每一个流长有若干条不同的流,在流长较长处可能在很长一个区间才出现一条流.

由于图 2 的横、纵轴坐标都取对数为计数单位,五角星标记表明平均速率均值随流长的增加而减小,呈现大致的线性下降关系,流长较短的流为慢流的可能性比较大,而长流基本上为快流;正方形表示的方差也有类似线性下降关系,只是这种关系没有均值分布那样明显,可以推测快流报文到达时间的方差相对慢流要小一些;三角形标记的偏差系数则呈现一种比前两者更加模糊的线性增加的趋势,这正好与前两者的变化趋势相反,可以推测快流的拥塞程度比慢流的更加严重,慢流的流内报文到达速率比较平稳.

由此,关于流速测度,本文得出以下几点推论:

(1) 流内报文到达间隔是服从重尾分布的,绝大部分流的报文到达速率较大;

(2) 随着流长的增加,流平均报文达到速率(即流的平均流速)呈增长的趋势;

(3) 平均流速越大的流,其流速不稳定性也越明显.也就是说,快流存在突发的状况比较严重,由于流内平均速率较大,所以每次突发传递的报文数比较多;

(4) 平均流速较小的流,其流内报文到达速率比较平稳.

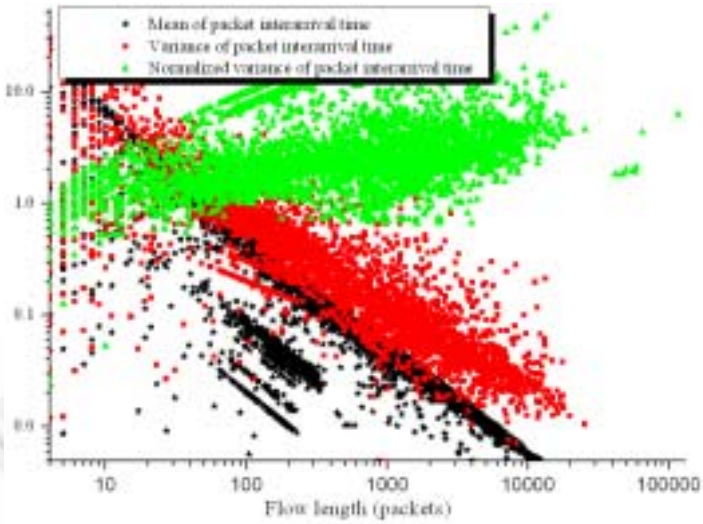

Fig 2 Flow rate stability analysis based on variance of packet interarrival

图 2 基于流内报文到达时间方差的流速平稳性分析

2.2 短流和长流首部报文的流速测度特性分析

由于短流占据了流总数的很大比例,分析短流的到达速率特点,对流识别中超时的设定有较大的影响.本文对短流的流速测度特性进行考察,表 1 是从 CERNET 华东北地区主干网络,在不同时刻采集的使用五元组流规范 64s 固定超时(以下所有测试采用的流定义方式除非特殊说明,否则都是采用该方式)定义的 500 000 个短流(共 5×500000 个短流),对其持续时间所占比例进行统计分析的结果(其中:栏为时间段,列为不同时段).从持续时间数据比较分析可以看出:不同时段的短流持续时间在各个区段的比例大致相同,而且绝大部分(超过 95%)短流的持续时间小于 16s.从不同网络中采集的数据进行分析,如果使用 5 元组的流识别方式,绝大部分流属于短流,传统的流识别策略对报文的处理都是采用 64s 的超时策略,这样就使得大部分资源没有得到有效的利用.

Table 1 The ratio of duration for short flows (Packetnum<6)

表 1 短流(Packetnum<6)持续时间的比例

	$t<2$	$2\le t<4$	$4\le t<8$	$8\le t<16$	$t\ge16$
2004_04_17_00:00	0.327	0.127	0.396	0.209	0.041
2004_04_17_04:00	0.317	0.099	0.289	0.271	0.032
2004_04_17_08:00	0.467	0.115	0.202	0.177	0.039
2004_04_17_16:00	0.467	0.130	0.223	0.126	0.051
2004_04_17_20:00	0.424	0.122	0.277	0.127	0.060

另外,本文还考察了来自相同数据集共 1 000 000 个长流的前 N 个报文到达时间的比例分布情况,见表 2(其中,栏为报文数,列为时间段).从总体上看:随着 N 值的增大,到达时间在各个时间段内变化的趋势幅度比较小,特别是大于 16s 的流所占比例只是缓慢增长,其中主要原因可以由上文所得的推论来解释:一般来说,长流的流内平均报文到达速率较快,也存在比较严重的突发现象,只有在长流属于慢流或者长快流的前 N 个报文中出现一个或多个突发间隔时,才会出现前 N 个报文到达时间超过 16s 的情况.

Table 2 Interarrival time of first N packets

表 2 前 N 个报文到达时间

	2	3	4	5
$t<2$	0.432	0.412	0.390	0.229
$2\le t<4$	0.385	0.320	0.262	0.288
$4\le t<8$	0.126	0.207	0.201	0.205
$8\le t<16$	0.040	0.028	0.106	0.133
$t\ge16$	0.017	0.033	0.041	0.045

通过以上关于报文数<6 的短流和长流前 5 个报文到达时间的分析,本文得出以下推论:短流或者长流的前 5 个报文到达时间都是比较小的,快流占流总数的绝大部分,其中短快流所占的比例也比较大.Zhang,Breslau 等人[2]针对其他网络分析的结果也证明了这一点.

3 基于流速特性的动态超时策略(DToS)

通过流规范和超时定义的流所表现出的特性,完全取决于特定的流规范和所选用的超时策略,因此,同一网络中采用不同流规范和(或)超时机制得到的流特性存在很大的差异.但是,使用相同的流定义规范而使用不同的超时策略,却可以在保证流识别精度的前提下大幅度减少流识别所需的系统资源.

3.1 DToS策略的提出

本文根据网络流量状况,针对流的不同到达报文速率特性和流长特性采用动态超时策略(DToS),可以在基本不影响流识别精度的情况下,大幅度地提高流测量资源的利用效率.DToS 策略利用网络流速测度特性的分析结果,采用动态超时的方式识别不同速率特征的流,尽快发现已经终结的流并将其从运行空间中清除,从而使测量系统的资源利用得以最优化.DToS 策略的工作原理图如图 3 所示.

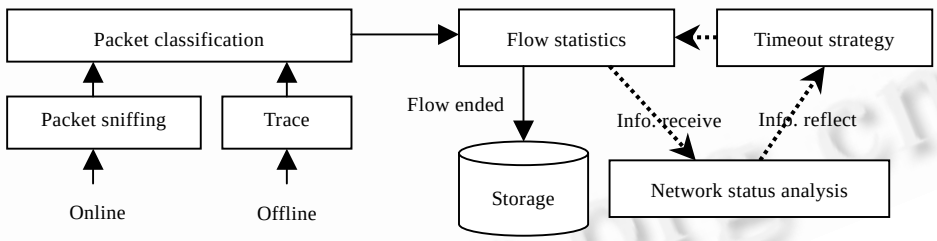

Fig.3 The working flow structure using DToS algorithm

图 3 DToS 策略工作原理图

首先设定若干初始值,短流:流包含报文数≤N;短流超时时间阈值:T_S;短流持续时间阈值:T_{SD};长流超时时间阈值:T_L;流数量和报文数量比例阈值:ξ.

(1) 当一个报文到达时,通过报文分类器为新到报文在流分析空间中创建新流或者将该报文归入特定的流中;对报文数>N 的流,对 TCP 流采用协议分析(TCP 的 FIN 标志位)结合固定超时,通过 FIN 标志位定义一个 TCP 流的终结,对非 TCP 流采用 MBET 策略,为每个非 TCP 流维护一个动态的超时[1];

(2) 使用值为 T_S 的时间间隔定时扫描流分析空间,如果发现流长≤N 且持续时间≤T_{SD},最后一个报文到达时间超过 T_S 时,则认为其已经终结,并将其从流分析空间清除;对采用 MBET 策略的流采用各自的保存的超时将其从流分析空间清除;对在内存中已长期存在且未接收到 FIN 的长 TCP 流采用固定超时 T_L 将其从流分析空间清除;

(3) 网络状况分析模块在每次扫描流分析空间时,获取单位时间段内新建流数 F 和新到报文数量 P,如果 $F/P>\xi$,则调整相关参数:$T_S=T_S/2$,发出流异常报警.

由于网络状况各不相同,所以 DToS 策略中所涉及的参数需要根据网络具体状况进行设置和调整.在一般网络中,N 为短流长度阈值,推荐为 5;T_S 的推荐值为 16s;T_{SD} 根据短流的长度而改变,推荐值为 $packetnum\times T_S/N$,

其中 *packetnum* 为该短流实际流长;T_L 为长流超时阈值,一般设置为 64s;ξ的取值主要与网络中平均流长和异常的定义存在较大的关系,平均流长 L 可以通过一段时间的测量获得,一个特定网络中在正常情况下平均流长并不随时间变化发生剧烈变化,由于在宏观角度分析网络异常一般是由大规模的短流组成,因此将本次扫描所获平均流长与上一个扫描所得平均流长的比值小于β称为异常,此时可以得到$\xi=1/(L\times\beta)$,例如某网络平均流长 $L=40$,并设$\beta=0.75$,则阈值$\xi=1/30$.

3.2 DToS策略性能分析

相对其他流超时策略而言,DToS 策略需要额外计算开销用于判断和推测每个流的长度,并为每个流动态设置超时不同的超时时间,因此,建立策略的代价模型可以为整个策略性能的评估提供可量化的指标.本策略主要涉及的几个参数包括:创建每个流所需时间 C_{CF}、单位时间维护每个短流所需计算时间 C_K(主要用于扫描流空间时查看每个流是否超时,单位时间扫描流空间次数为α)、判断流长度所需计算资源 C_{FL}、维护每个流平均使用存储空间 S_F.假设短流在总体流中所占的比例为μ,短流平均超时为 T_S,长流平均超时为 T_L;固定超时策略每个流的超时为 T_L.

采用固定超时方式和 DToS 策略平均创建并维护一个流所使用的计算资源分别为公式(1)和公式(2).

$$F_{C1}=C_{CF}+\alpha\cdot T_L\cdot C_K \tag{1}$$

$$F_{C2}=C_{CF}+C_{FL}+\mu\cdot\alpha\cdot T_S\cdot C_K+(1-\mu)\cdot\alpha\cdot T_L\cdot C_K \tag{2}$$

由于 $T-T_S>0$,故由公式(1)、公式(2)比较可以得出以下结论:

$$\mathrm{MAX}(F_{C2}-F_{C1})=C_{FL} \tag{3}$$

由于判断每个流超时时间的计算复杂度为 $O(1)$,所以 DToS 策略在每个流的计算时间上相对固定超时策略并没有显著的增加,从后文第 4 节实验结果分析可知,计算时间大概增加了 5%左右.

采用固定超时方式和 DToS 策略平均创建并维护一个流所使用的存储资源分别为 $T_L\cdot S_F$ 和$\mu\cdot T_S S_F+(1-\mu)\cdot T_L S_F$,则维护每个流所需存储资源,DToS 策略所节省的空间为$\mu\cdot(T_L-T_S)\cdot S_F$.由于网络中短流的数量占大部分,也就是说,$\mu$接近于 1,而且在实际测量中,$T_S$ 的取值远小于 T_L,所以,DToS 在存储资源利用性能上比传统的固定超时策略有显著的提高.

在识别短流并设置其超时时,还增加了一个判断条件——短流持续时间阈值 T_{SD}.这主要基于流速测度的特性考察,从图 1 流内报文到达速率及其平稳性分析结果可以看出:相对快流而言,慢流较少但平稳性较好.通过设置短流持续时间阈值,可以防止一部分慢流被系统误认为短流并截断,进一步保证了测量的精度.

当流与报文比例值突然增加并超过阈值ξ时,表明被测网络中短流数量急剧增加,这种现象是 DDoS 攻击和蠕虫爆发等网络异常比较典型的特征.由于网络中流数量的急剧增加,采用固定超时、MBET 以及基于协议和内存控制等超时策略的测量系统都没有针对这种异常情况的应急方案,可能会导致内存耗尽进而影响测量精度,甚至导致测量系统的崩溃.DToS 策略针对这种异常情况,通过减小短流的超时时间,使短流尽快被识别并从内存中清除,以少量且可控的精度损失为代价,保证测量系统的正常运行.

3.3 DToS策略误差分析

DToS 策略在引入极少量计算消耗下,大幅度地减小了流测量系统存储资源的开销,但由于对大部分流使用较短的超时,出现将一些未终结的流误判为已终结的现象是不可避免的.本文以下部分就 DToS 策略在流识别精度上可能产生的误差进行详细的分析.

首先,假设所有流的流内报文到达时间间隔 X 相互独立且服从同一分布,分布函数为 $F(x)$,概率密度函数为 $f(x)$,Y 表示一个流前 n 个报文所需到达时间,其分布函数为 $F(y)$,概率密度函数为 $f(y)$,则:

$$Y=\sum_{i=1}^{n-1}X_i,\ n=2,3,\ldots$$

$$F(y)=F\left(\sum_{i=1}^{n-1}x_i\right)=\int_{-\infty}^{+\infty}f(y)\mathrm{d}y.$$

由多元分布统计相关定理可知:多元累加的概率密度函数等于其包含每个变量密度函数的卷积,即

$$f(y)=f(x_1)\times f(x_1)\times\ldots\times f(x_N).$$

然后,考察流间报文到达时间间隔服从何种分布.采用第 2 节流速测度分析的数据集,图 4 描述了两类流的流内报文到达时间间隔,第 1 类是随机选取的流长大于 6 个报文的 20 000 个流(normal flow),第 2 类是随机选取的流长大于 6 个报文且平均报文到达时间间隔小于 0.1s 的 20 000 个流(quick flow).从这两类流的报文到达间隔累积分布曲线来分析,当时间间隔取值为≥1s 时(只考虑报文到达间隔≥1s,是由于在短流超时 T_S>>1s 的情况下,小于 1s 的报文到达间隔对流测量结果精度的影响可以忽略不计),到达时间间隔均大致服从参数为 λ=0.103,α=−0.93 的 Weibull 分布,其中:前一种流累积分布曲线略低于 Weibull 累积分布曲线;后一种流累积分布曲线略高于 Weibull 曲线.

$$f_{X_i}(x)=\begin{cases}\alpha\lambda x^{\alpha-1}\mathrm{e}^{-\lambda x^{\alpha}}, & x>0,\\ 0, & x\le 0,\end{cases}\quad i=1,2,...,n.$$

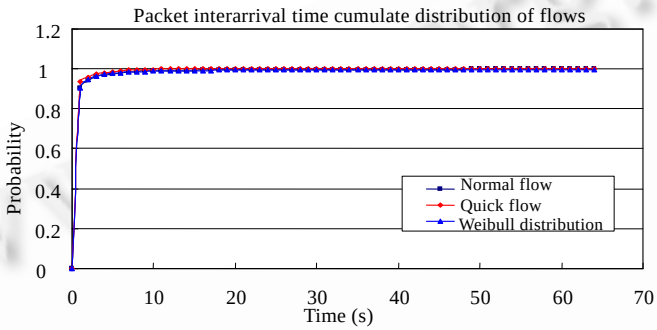

Fig.4 The CDF curve of packets interarrival time of different types flows

图 4 流内报文到达时间间隔累积分布(CDF)曲线

接下来考虑前 N+1 个报文到达所需时间的分布情况,由于计算 f_Y 十分复杂,本文采用一种简化的方法.从到达时间间隔的分布曲线在间隔≥1 时基本服从 Weibull 分布可以得出以下定律:

定律 **1**. 随着到达时间的增加,在该时段内到达报文的数量逐渐减小,而且报文数减小的幅度也逐渐减小.

由定律 1,本文作以下假设:

假设. N 个报文到达时间最长的情况,也就是 N 个报文到达时间≤T 的可能性最小的情况,是这 N 个报文的到达时间间隔均相等时:$t_1=t_2=\ldots=t_{N-1}=T/(N-1)$.

证明:设 N 个报文的到达时间分别为 $t_1,t_2,\ldots,t_{N-1}$,由于到达时间总长和到达的顺序无关,所以在不失去一般性的前提下,定义:$t_1\le t_2\le\ldots\le t_{N-1}$;设 T 为前 N 个报文到达所需时间;$P(t_i)$为到达时间<t_i 的报文数占报文总量的比例;$F(t_i)$为时间点 t_i 的分布函数,即累积密度函数,$P(t_i)=1-F(t_i)$;$P_N(T)$为前 N 个报文到达时间小于 T 的可能性;则

$$T=t_1+t_2+\ldots+t_{N-1},\ P_N(T)=\prod_{i=1}^{n}P(t_i)=\prod_{i=1}^{n}(1-F(t_i)).$$

由定律 1 和假设条件可知:

$$F(t_1)\ge F(t_2)\ge\ldots\ge F(t_{N-1})\text{且 }F(t_2)-F(t_1)\ge F(t_3)-F(t_2)\ge\ldots\ge F(t_{N-1})-F(t_{N-2}).$$

当 T 为固定值时,根据单调递减函数的性质,只有当 $t_1=t_2=\ldots.=t_{N-1}=T/N$ 时,$P_N(T)$存在最小值为

$$\mathrm{Min}(P_N(T))=(1-F(t))^{N-1},\text{当}t_i=t=T/(N-1),\ i=1,...,N-1.$$ □

从以上证明结论可知:对所有长度大于 N 的流而言,前 N 个报文到达时间小于 T 占所有流的比例的最小值为$(1-F(T/(N-1)))^N$,其中 $F(T/(N-1))$为 Weibull 累积分布曲线在 $T/(N-1)$处的取值.

在实际测量中,T 取值为 T_S=16s,N 取值为 5,可以通过查询 Weibull 累积分布曲线得到 $F(T_S/(N-1))=F(4)=0.028$,则 $\mathrm{Min}(P_N(T_S))=(1-0.028)^4=0.90$.图 4 对快流累积分布曲线考察的结果显示 $F(T_S/(N-1))=0.012$,重新计算 $\mathrm{Min}(P_N(T_S))=(1-0.012)^4=0.953$.

采用 Mitchell.T.M.在文献[11]中提出的计算离散值真实错误率假设的置信区间的方法:

$$error_p(h)=\left[error_S(h)\pm z_N\sqrt{\frac{error_S(h)(1-error_S(h))}{n}}\right],$$

其中,$error_S(h)$是样本错误率,即错误样例所占的比率;z_N是与置信度相关的常量;n为所选取的样本数.

取置信度为99%,对应的z_N为2.58;n值为20 000;$error_S(h)$=1–0.953=0.047.计算真实错误率$error_D(h)$的99%置信区间:

$$error_p(h)=\left[0.047\pm 2.58\sqrt{\frac{0.047\cdot(1-0.047)}{20000}}\right]=[0.047\pm 0.00384].$$

因此可以得出如下结论:考虑使用参数对T_{SD}对流超时识别在精度上的保证,在最差情况下,采用DToS超时策略的流测量系统将长流截断的可能性小于5%.本文第4节中给出的实际测量的结果显示,本策略的误差远小于理论计算的最差情况.

4 测量实验结果

由本文开始部分给出的流定义可知:在相同流规范约束下,流识别的主要差异也就是其识别精度主要取决于使用的超时策略.本文针对2004年4月某日采集自CERNET主干华东北节点历时1小时的TRACE,使用相同的流规范(五元组定义方式),不同超时策略(传统固定超时策略[4,5]、MBET超时策略[1]和DToS策略)进行测试,所观测到的流累积分布曲线和内存中活动流数量的曲线如图5和图6左图所示.

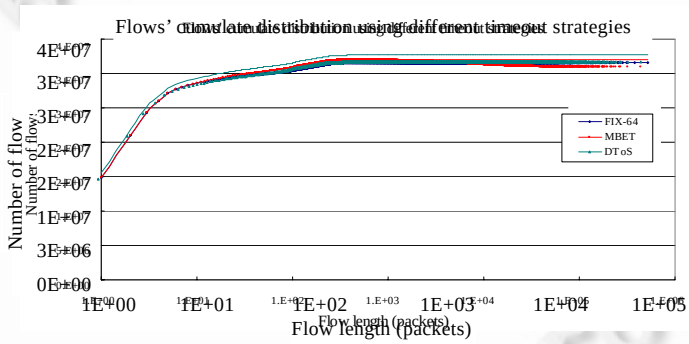

Fig.5 Flow number CDF curves using different kinds of timeout strategies

图5 采用不同超时策略的流累积分布(CDF)曲线

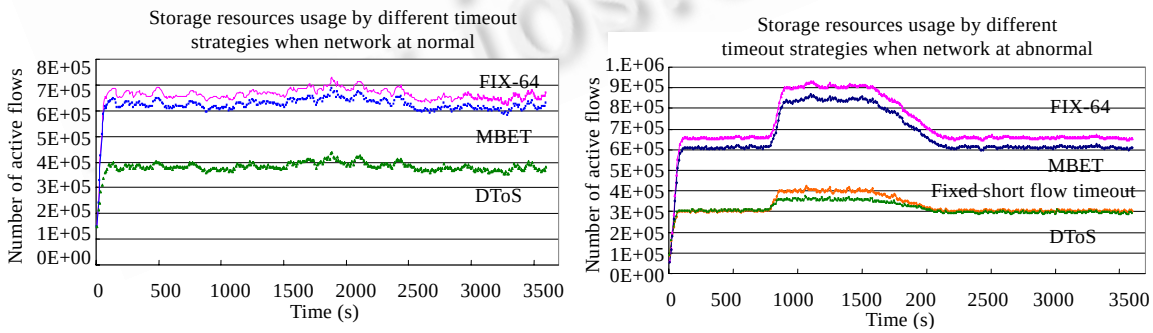

Fig.6 Flow number CDF curves using different kinds of timeout strategies

图6 不同状况下各种超时策略资源使用情况对比

固定超时策略采用的超时为64s(FIX-64);MBET超时策略采用的输入参数为T_0=4,S=5,P={21,18,15,12, 9},则其$T_{MAX}=T_0\times 2^{5-1}$=64,即其初始超时值为64s;DToS策略参数定义如下:流长分界N=5,短流超时T_S为16s,短流持续时间阈值$T_{SD}=packetnum\times T_S/N$,长流超时为$T_L$为64s,$\xi$为1/16(本文所测得的CERNET主干中双向流在正

常情况下平均流长为 20 个报文左右,ξ取值为 1/16 表示在流平均长度为 16 时,即当流数量增加 25%时启动相关操作).

根据图 5 相关流累积分布曲线可知,采用不同超时策略所观测到的数据流绝大部分情况下在数量上是相等或者近似相等的.这表明了这 3 种不同的超时策略在实际测量中在识别精度方面只存在微小的差异.也就说明,通过实际测量获得的流速特性对流的超时机制进行优化,只要选择正确的参数,对流识别正确性几乎没有影响.

总体而言,使用 DToS 策略所得流总数略高于 MBET 策略;而 MBET 策略所得流总数略高于固定 64s 超时策略.而且三者的差异主要集中于短流数量.主要原因在于:部分在首部存在突发间隔的流被截断成两条,突发情况比较严重的流可能被截成多条流,因此实际受影响的流的数量很小.本文通过对来自 CERNET 网络中随机抽取的 10 000 条长流进行监测,实验数据显示:相对 64s 固定超时而言,只有 0.57%的长流受到 DToS 策略影响而产生被截断的现象,而且这些流的平均流内报文到达时间基本都小于长流的平均流内报文到达时间.因此可以得出以下结论:DToS 策略对流识别精度特别是流速较快的流的识别精度影响很小,在大多数情况下基本上可以忽略.另外,由于 DToS 策略中引入了利用协议分析判断流是否结束的机制,可以在相同条件下对流识别的正确性有所改进.

图 6 左图显示了在正常情况下,不同超时策略所对应在内存中活动流的数量.由于在流分析中,每个流所占用的内存空间基本相同,所以活动流数量直接对应系统所占存储空间数.从图中不同超时策略对比的情况可以看出:DToS 所占用空间的数量大约为固定 64s 超时策略的 54%,MBET 超时策略的 62%.也就是说,在正常情况下,DToS 策略可以比其他策略节省大约 40%的存储空间.

图 6 右图描述了在异常情况下,采用不同超时策略的测量系统在内存中维护活动流的数量,数据是基于 CERNET 流速测度特性和活动流等情况模拟而得.相关参数为:正常情况平均每秒新到流数量为 10 700,流和报文数比例为 50.当系统运行 800s 附近时,流数量开始显著增加,这些增加的流 99%以上是短快流,增加幅度达到 40%,并持续 800s 左右时间开始逐渐减小,大概在 2 300s 左右恢复正常.从曲线对比可以看出:固定 64s 超时和 MBET 策略维护活动流数目平均增加了 35%以上,而 DToS 策略活动流数量在未采用应急措施的情况下,其增加值只有前两者的 1/4,在使用阈值ξ判断流数量增加比例并应用动态超时策略时,实际流数目增加值稍高于前两者的 1/8.由此可以看出,DToS 策略在应对网络中出现异常,流数量急剧增加的情况,相对其他几种超时策略具有明显的优势.

5 结论及展望

随着网络带宽的不断提高(OC48,OC192 等),网络数据流量的不断增长,提高组流的效率已经成为基于流粒度网络行为分析最重要和急需解决的问题之一.本文通过详细分析现有流超时机制,指出它们应用于目前网络流识别时存在的不足之处;基于 CERNET 主干华东北地区节点,对不同时段经过主干数据报文的详细分析,对流的流速测度各项指标进行了比较完整的考察,分析总结了高速网络中流速测度的特征;在流识别超时机制剖析和流速测度特征分析的基础上,本文提出了一种高速网络中基于流速测度特征的动态超时策略——DToS 策略,该策略可以根据网络的运行状况和流速特性,针对不同流速特征的流动态改变该流的超时,从而在基本不损害流识别精度的前提下,尽可能地减小流识别所需的系统资源;并在理论上对 DToS 策略的性能和误差进行细致的分析和证明,论证了策略的可行性;最后通过观测不同时段 CERNET 主干流量,经过实验验证了策略的性能和误差,并进一步验证了策略的可行性,为深入进行流行为的分析提供了必要支持.

针对同一个测量对象,将使用 DToS 策略的获得测量数据与其他两种目前普遍使用的超时策略所获测量数据相比较,结果显示,DToS 策略在测量所需消耗的资源上均优于这两种策略,只有后者的 1/2 左右.特别是在网络出现异常时,短流的数量将急剧增加,现有超时策略不能应对这种突发状况,可能因为系统资源的耗尽而影响测量的精度甚至导致测量系统崩溃;DToS 通过对流量实时监测及时发现这种现象并采用动态超时优化处理被测网络中存在的异常流,使其能被尽快淘汰.通过对模拟数据测量结果显示,随着异常流的增长,DToS 策略存储资

源占用提高的幅度仅略高于其他两种策略的 1/8,从而有效地减小了资源的消耗,保证了测量的正常进行.

DToS 超时策略虽然有效地解决了短流超时的优化处理问题,并根据流速测度特性提出了优化提高流测量系统中流识别的精度,但由于在短流超时的减小不可避免会导致一些存在突发的长流被截断,从而导致流识别的精度有略微降低(第 3.3 节通过理论证明精度降低可以控制在一定的范围内).由于五元组方式的流识别机制对流考察是建立在 TCP 层基础上的,而没有对高层协议相关内容进一步探讨,所以也就不能支持通过高层协议对网络行为的分析,这是本文未来的研究方向.

References:

[1] Ryu B, Cheney D, Braun HW. Internet flow characterization: adaptive timeout strategy and statistical modeling. In: Workshop on Passive and Active Measurement (PAM), 2001. Amsterdam: RIPE Network Coordination Center, 2001. http://www.ripe.net/pam2001/

[2] Zhang Y, Breslau L, Paxson V, Shenker S. On the characteristics and origins of Internet flow rates. In: Proc. of the ACM SIGCOMM 2002. Pittsburgh: ACM Press, 2002. 309–322. http://citeseer.ist.psu.edu/zhang02characteristics.html

[3] Iannaccone G, Diot C, Graham I, McKeown N. Monitoring very high speed links. In: Internet Measurement Workshop 2001. San Francisco, ACM Press, 2002. 267–271. http://www.imconf.net/imw-2001/imw2001-papers/63.pdf

[4] Claffy KC. Internet traffic characterization [Ph.D. Thesis]. San Diego: University of California, 1994.

[5] Claffy KC, Braun HW, Polyzos GC. A parameterizable methodology for Internet traffic flow profiling. IEEE Journal on Selected Areas In Communications, 1995,12(8):1481–1494.

[6] Wang JF, Li L, Sun FC, Zhou MT. A probability-guaranteed adaptive timeout algorithm for high-speed network flow detection. Computer Networks, 2005,48(2):215–233.

[7] Hohn N, Veitch D. Inverting sampled traffic. In: Proc. of the 3rd ACM SIGCOMM Conf. on Internet Measurement. 2003. 222–233. http://www.imconf.net/imc-2003/papers/thinning1.pdf

[8] Guo L, Matta I. The war between mice and elephants. Technical Report, BU-CS-2001-005, Boston University, 2001. http://www.cs.bu.edu/techreports/2001-005-war-tcp-rio.ps.Z

[9] Yilmaz S, Matta I. On class-based isolation of UDP, short-lived and long-lived TCP flows. Technical Report, BU-CS-2001-011, Boston University, 2001. http://www.cs.bu.edu/techreports/pdf/2001-011-cbi.pdf

[10] Rey M. Transmission control protocol. RFC793, 1981. http://www.faqs.org/rfcs/rfc793.html

[11] Mitchell TM. Machine Learning. Beijing: China Machine Press, 2003. 96–99 (in Chinese).

附中文参考文献:

[11] Mitchell T.机器学习.北京:机械工业出版社,2003.96–99.

周明中(1976－),男,江苏宜兴人,主要研究领域为网络行为学.

丁伟(1963－),女,教授,博士生导师,主要研究领域为网络体系结构,网络安全,网络行为学.

龚俭(1957－),男,教授,博士生导师,CCF 高级会员,主要研究领域为网络体系结构,网络安全,网络行为学.