

# 网络流超时策略研究<sup>1</sup>

周明中 龚俭 丁伟

(东南大学计算机系 江苏南京 210096)

(江苏省计算机网络技术重点实验室)

**摘要:** 基于流特性的测量在网络行为分析中发挥越来越重要的作用。超时策略作为流识别的主要标志之一, 对流特性测量的正确性和性能有很重要的影响。本文通过对现有流超时策略进行比较和分析, 指出适用范围和存在的问题。针对单包流占总体流量很大比例的特点, 本文提出了两层自适应超时策略 (TSAT)。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, 提高了测量系统的资源利用率。最后通过实验论证本文提出的超时策略在实际测量中的性能, 并进一步分析适用范围。

**关键词:** TSAT 策略; 网络数据流; 超时策略; 流特性

中图分类号: TP393

文献标识码: A

文章编号:

## Study of Network Flow Timeout Strategy

ZHOU Ming-zhong, GONG Jian, DING Wei

(Department of Computer Science, Southeast Univ., Jiangsu, Nanjing 210096 China)

(Jiangsu Province Key Laboratory of Computer Networking Technology)

**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 discussed the state-of-art of flow timeout strategies, and pointed out where they were applicable and their shortcomings. The paper presented a Two-level Self-Adaptive Timeout (TSAT) strategy which handles flows with different timeout strategy according to its feature. This method could improve the performances of network measurement and the efficiency of the resource usage of measurement systems. Some experiments were employed to show the rationality of TSAT strategy. Then the fitness area of strategy was anatomized as well in the paper.

**Key words:** TSAT strategy; network flow; timeout strategy; flow characteristics

### 1 引言

随着 Internet 的发展及其用户的增加, 网络流量变得越来越大, 网络行为也变得越来越复杂。针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的措施, 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。数据包 (packets) 是网络中最小的传输单元, 其特性比较明显而且容易察觉。最初网络行为研究主要集中在数据分组层次上, 但由于这些研究相对平等地分析每个数据包, 从而导致对包间关系及其更高层次信息分析的缺失。

针对流的网络行为研究在很多方面弥补了局限于数据包层次研究的不足。所谓数据流, 是指符合特定的流规范 (specification) 和超时 (timeout) 约束的一系列数据包的集合[3], 对同一个数据包序列, 不同的流规范和超时机制可以得到不同流的集合。对数据流的分析和整形 (profiling) 可以提高整个网络的性能和网络的服务质量。

使用五元组定义流的方式被广泛地采用[2][3][6], 其主要测度参数包括: 流规模, 流大小分布, 到达时间间隔等。为了便于介绍, 在不引起歧义的情况下, 引入 Ryu 在[3]中提出的根据包含包数量区分流的概念, 并根据 CERNET 流分布的实际情况将流分为单包流/短流/长流(SP/S/L): 单包流是指只包含一个数据包的流, 短流是指数据包数量等于或小于 10 个的流, 其余的流均看作长流。

本文的第二部分分析和比较了现有超时策略及其它们在流识别中存在的不足, 第三部分根据 CERNET 流量观测分析的结果, 提出两层自适应超时算法 (TSAT), 并将其性能与其他超时算法进行比较和分析, 通过实验论证其可行性。

<sup>1</sup> 本文受国家 973 计划课题 (2003CB314803) 资助

## 2 超时策略分析

超时是流识别的重要标志之一，不同超时对观测流的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过长时间地占用存储空间，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）。所以目前超时研究的主要方向是根据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。

K. C. Claffy[1]提出了采用固定超时实现的方法，并通过实验证明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的包到达速率的流，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 Timeout 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 64 秒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的偏差甚至错误。

B.Rye, D.Cheney,et al.在[3]中提出的 MBET 算法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。该算法在新流建立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的流吞吐量，以维持或 2 的指数形式递减超时的值，从而在尽量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（尽快地使已结束的流从内存中清除）。但该算法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特点，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。

N.Hohn, D.Veitch[7]在此基础上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相结合，在必要时为保证测量性能必须牺牲其正确性。

在[1][2][3]中的测量数据表明，在不同网络中均存在大量的单包流，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，单包流的个数占网络流总量的 40% 以上。这些单包流对流的总体分布和流的特性有很重要的影响，同时也在流识别过程中占用了大量的系统资源。现有的超时策略都没有对此作优化处理，导致这些单包流和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，单包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 攻击或蠕虫爆发时），单包流在流总量的比例将急剧上升，其所消耗的资源也将相应增加，如果不对单包流做优化处理，可能导致资源耗尽，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少地使用系统资源。现有流分类和识别方法一般都使用单一的超时判断机制[2][3][7][8]，在判断精度和性能上各有千秋，但均不能最大可能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，以便在保证流的识别精度条件下更合理地使用系统的资源。

## 3 两层自适应超时策略（TSAT）

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有很大的差异。引言已明确定义了本文所讨论流的规范，本节在特定流规范下，结合 CERNET 流特性，提出了两层自适应超时策略（TSAT），使用不同方式区别对待不同特性的流，以达到有效利用系统资源的目的。

### 3.1 策略的提出

两层自适应超时策略通过设置两层超时机制区别对待不同特性的流，以尽可能较早发现和淘汰已经结束的流。具体策略是结合固定超时策略和自适应超时策略的优点，利用固定超时发现单包流，并将其剔除；对剩余的流采用自适应策略在保证流识别正确性的基础上提高性能，节省存储空间。其主要步骤如下：

（1）创建两个存储空间：一个用于暂存新到且不属于特定流的数据包，称为单包空间；另一个用于维

护流信息，称为流信息空间。

- (2) 单包空间和流信息空间采用不同的超时机制，单包空间采用固定超时策略，将其超时设为  $T$ ，而流信息空间则结合协议判断，固定超时和 MBET 策略，为节省计算资源，单包空间先不为数据包创建流，直到淘汰该数据包时才作相关流信息提取。
- (3) 对每一个新到来的包检查其是否属于流信息空间维护的某一个特定的流，如是则更新相关流信息。
- (4) 否则检查单包空间是否存在与该包属于同一个流的数据包，如存在则创建一个新流并在流信息空间维护其相关信息；如不存在则在单包空间维护该数据包的信息。
- (5) 定时扫描单包空间和流数据空间（两者扫描的时间间隔相互独立），如单包空间维护的包存在的时间达到固定超时  $T$  时，将其从单包空间中清除；流数据空间中流对 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，对在内存中已长期存在且未接收到 FIN 的流采用固定超时将其淘汰；对非 TCP 流采用 MBET 策略，为每个非 TCP 流维护一个动态的超时[3]，每次扫描也可以将已终结的流清除出去。

TSAT 对现有流超时机制的主要改进在于针对网络中流的分布和特性，引入了两种超时机制，分别处理单包流、短流和长流，以达到更有效地维护流信息的目的，其中短时间粒度固定超时机制主要针对单包流，协议分析、长时间粒度的固定超时和 MBET 机制适用于其他流。实验显示在 CERNET 主干网中，单包流在网络总体流中所占的比例在 40% 以上，采用比较简单且准确有效的方法尽早发现和终结这些单包流，然后采用各种超时机制结合优化的方法处理非单包流，可以在保证流识别正确性的前提下，提高系统的处理效率，使系统资源利用达到最优化。

### 3.2 TSAT 算法性能分析

单包空间一般采用较小的固定超时，这是建立在非单包流的第一个包到达时间 (FIT) 基本均小于该固定超时基础上的。这样才能保证绝大部分流不被截断。对 CERNET 不同时间段的流观测，结果显示大约 95% 以上非单包流的 FIT 在 8 秒以内，如果将时间间隔衡量扩展为 16 秒则该比例将扩展为 99% 以上。

表 1 是从采用 64 秒固定超时的观测数据中随机抽取 1,000,000 条不同长度非单包流，并根据其第一个包到达时间分类的结果。其中横栏表示流包含的包数量（即流长），纵栏表示到达时间的范围，表中数据表示针对随机选出的流根据到来时间和流长进行分类统计的结果。这些数据显示一半以上的流（53.53%）的 FIT 在 2 秒以内，位于 8 秒内的 FIT 也占 89.47%，而 97.19% 的 FIT 集中在 16 秒以内；表 2 的数据还进一步验证了实验观测所得的流量分布情况；从不同流长的 FIT 分布来看，一般流越长则其平均 FIT 就越小，譬如包数大于 100 的流的 FIT 绝大部分均小于 2。

表 1 不同规模非单包流第一个包达到时间分布比较表

	$X \leq 10$	$10 < X \leq 100$	$100 < X \leq 1000$	$> 1000$
$T \leq 2$	389356	89804	55472	692
$2 < T \leq 4$	246162	9573	655	29
$4 < T \leq 8$	98426	4399	185	1
$8 < T \leq 16$	75201	1924	92	3
$16 < T \leq 32$	11355	952	30	3
$32 < T \leq 64$	15178	491	17	0

本文利用评估假设来检验 FIT 为 16 秒这个假设的精度，通过计算样本错误率来估计真实错误率，采用 T.M.Mitchell 在[5]中提出的计算离散值真实错误率假设的置信区间的方法：

$$\left[ error_s(h) \pm z_N \sqrt{\frac{error_s(h)(1 - error_s(h))}{n}} \right]$$

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。

根据表 1 数据可知， $error_s(h)$  为 FIT 超过 16 秒流所占的比例，其值为 28026/1000000；本文取置信

度为 99%，对应  $z_N$  为 2.58； $n$  值为 1000000。计算真实错误率  $error_D(h)$  的 99% 置信区间：

$$\left[ \frac{28026}{1000000} \pm 2.58 \sqrt{\frac{\frac{28026}{1000000} \left(1 - \frac{28026}{1000000}\right)}{1000000}} \right] = [0.028026 \pm 0.000165]$$

由于 16 秒 FIT 的流数量占总流数量的压倒多数，而通过假设检验证明该判断的真实错误率的 99% 置信区间也证明在单包空间采用较短的固定超时（如 16 秒），可以在极少量损失或不损失流识别正确性的前提下大幅度减小资源的消耗。

通过实验发现，绝大多数非单包流的第一个包到达时间间隔位于一个较小的时间范围内，所以一般将单包空间的固定超时设置为一个比较小的值，以较小的代价（极小部分流将被截断）来获取性能的改善，以下将通过建立算法的代价模型来论证性能的改善情况。

建立算法的代价模型可以为整个算法性能的评估提供可量化的指标，主要涉及的几个参数包括：为单包在单包空间创建相关信息平均所需的计算资源  $C_{SP}$ ；维护单包空间中每个数据包使用的平均计算资源  $S_{SP}$ （包括扫描与计算）和平均存储空间  $M_{SP}$ ；创建每个新流平均所需计算资源  $C_F$ ，维护每个流所使用的平均计算资源  $S_F$  和平均存储资源  $M_F$ 。假设单包流在总体流中所占的比例为  $\mu$ ，采用本文提出的算法平均创建和维护一个流所使用的资源分别为（1）和（2）：

$$mC_{SP} + (1 - m)(C_{SP} + C_F) \quad (1)$$

$$m(S_{SP} + M_{SP}) + (1 - m)(S_F + M_F) \quad (2)$$

假设在单位时间创建  $a$  个流，维护  $b$  个流状态，则考察该算法与传统超时算法代价，只需要验证式（3）是否成立：

$$a * (1) + b * (2) < aC_F + b(S_F + M_F) \quad (3)$$

由于单包空间一般采用较短的固定超时且其空间相对较小，所以可以保证  $M_{SP}$  和  $S_{SP}$  均要远小于  $M_F$  和  $S_F$ ，而当系统处于稳定状态时，单位时间内一般新建的流也远小于系统所维护的流（即  $a \ll b$ ），故上式必然成立。

对 CERNET 主干网的流分布情况进行分析的数据表明，任意时段内属于单包流的数据包占总数据包数的 0.5% 左右，绝大部分数据包归属于非单包流，所以单包空间相对较小，维护代价也相对较小。

非单包流采用协议分析、粗时间粒度的固定超时和 MBET 算法的结合，主要考虑 TCP 协议有明确的流结束标志，通过流结束标志识别流可以保证识别的正确性；粗时间粒度的固定超时可以保证在流出现异常（如 FIN 数据包丢失）时，将长期占用存储空间而没有接到结束标志的流清除出去。对于其他流，由于没有明确的结束标志，所以只能采用一般超时机制来判定流的结束，本文采用 MBET 算法，是因为通过对 CERNET 主干网中流间包到达速率进行抽样发现基本与 B.Rye, D.Cheney, et al. 在 [3] 中提出的包到达率分布情况相同。只需要选择合理的参数，它可以在保证流识别正确性的条件下，尽可能快地判断流的终结，并将其从内存中清除。

#### 4 相关实验

根据 B.Ryu 提出数据流的定义，在相同流定义下，流识别的主要差异源于不同的超时策略。本文对 2004 年 4 月 17 日 20 时—21 时 CERNET 主干流量采用不同的超时策略进行测试，所观测到的流分布曲线和内存维护流数量的曲线如图 1 和图 2 所示。

固定超时算法采用的超时为 64 秒（FIX-64）；MBET 超时算法采用的输入参数为  $T_0=4$ ， $S=5$ ， $P = \{21, 18, 15, 12, 9\}$ ，则其  $T_{MAX} = T_0 * 2^{5-1} = 64$ ，即其初始超时值为 64 秒；TSAT 算法分别对单包流空间采用 16 秒的固定超时（TSAT-SP 所示），对流信息空间的维护则采用自适应超时算法（TSAT-Flow 所示），

其中选用的参数：固定超时参数为 64 秒，MBET 算法参数与以上描述相同。

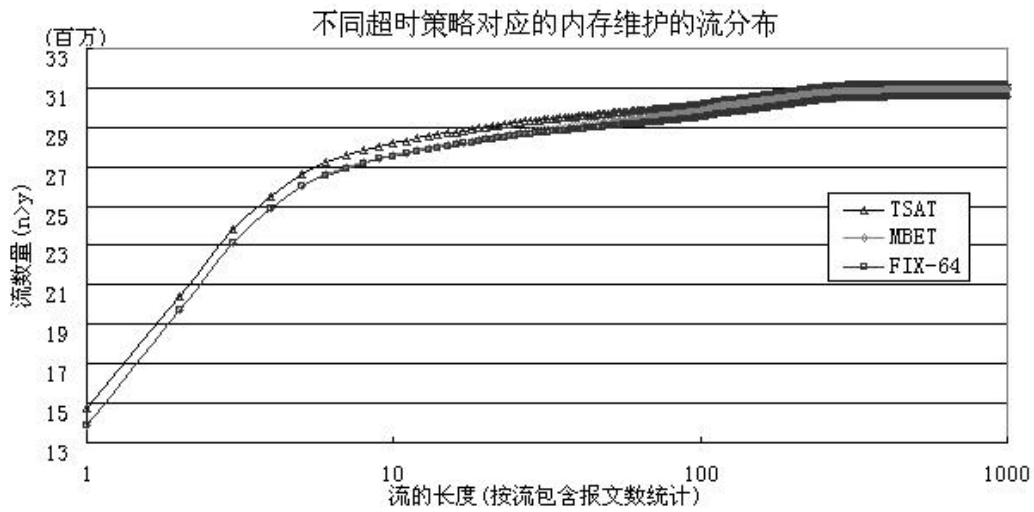


图 1 不同超时策略观测所得流分布曲线

图 1 有关曲线流分布曲线显示，总体而言采用不同超时策略所观测到的数据流的数目是基本相等的，这表明了采用 MBET 策略对流固定超时进行优化，只要选择正确的参数，对流识别正确性几乎没有影响，而由于 TSAT 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。采用减小单包流超时的策略不可避免地截断一部分非单包流，这也正是导致 TSAT 所观测到的流在数量上要略大于其他两种超时策略的原因，但由于被截断的流占流总数的比例很小（实验数据显示为 4.57%），且主要受影响的是慢速流（其中极慢速的流可能被多次截断），所以算法对流识别精度特别是快速流的识别影响很小。

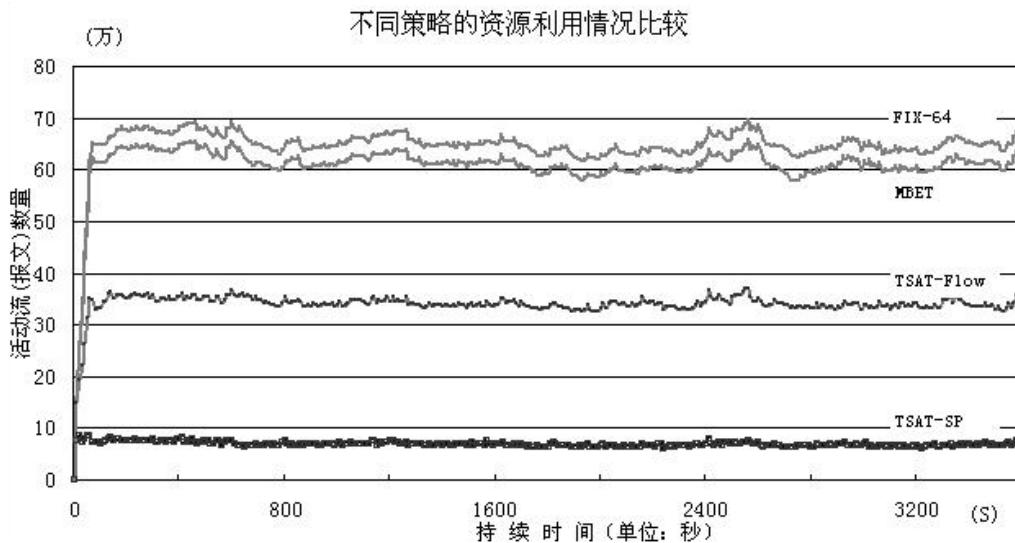


图 2 不同超时策略内存中维护流数量随时间变化比较曲线

图 2 是表现了相同规范定义的流采用不同的超时机制所得维护流数量的差异。从总体而言，固定超时算法，MBET 算法和 TSAT 算法所维护的流数量曲线随时间变化是相类似的，而在同一时间范围内，TSAT 所需维护流的数量是最少的，其所需计算和存储资源也是最少的。

从实验所得数据来看，由于采用动态超时策略，实际上其中有大部分非单包流的超时将减小（其相关的性能分析可以参考[3]），可以较早发现已经结束的流并将其清除出存储区域，所以其平均所需维护的流数要小于 FIX-64，但占其中接近 40% 的单包流的超时将维持初值，在初值较大的情况下，系统计算和存储资源的消耗是非常巨大的，故其对系统资源的利用并没有比 FIX-64 有明显的改善。

从图 2 的测试结果来看，单包空间是大约比流空间小一个数量级，而其相应流空间又只有 MBET 所维

护空间的 55%左右, 64 秒固定超时策略维护空间的 45%左右。维护单包空间所需的资源和流空间所需存储资源相比是微不足道的, 所以其所需系统的计算资源和存储资源均小远于目前普遍采用的两种超时策略。实验结果显示, 在正常情况下, 通过牺牲极小的流识别正确性, TSAT 策略所占用的系统存储和计算资源只有 MBET 策略和固定超时策略所占资源的一半左右。

## 5 结论和未来展望

基于流粒度的网络行为分析, 提出了在数据包层次之上对网络特性的刻画方式。研究流的分布和特性可以在数据包特性研究的基础上进一步揭示当前网络状况, 为具体的网络应用(如路由优化, MPLS 等)提供必要的技术支撑。

随着网络带宽的提高(OC48, OC192 等), 网络中数据包流量也不断增长, 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, 并以此为基础提出两层自适应超时策略: 第一层采用固定超时机制, 预先识别和淘汰单包流, 并将非单包流交给第二层作进一步处理; 第二层采用自适应超时机制, 及时发现和淘汰已经结束的流, 在基本不损失流测量正确性的前提下有效地节省了系统计算和存储资源。通过观测不同时段 CERNET 主干流量, 经过理论证明和实验验证论证了其可行性, 为进一步流行为的分析提供必要的支持。针对同一个测量对象, 将使用 TSAT 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 TSAT 算法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, 单包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; TSAT 通过及时发现和处理单包流, 并采用自适应算法处理非单包流, 有效地减小了资源的消耗, 保证测量的正常进行。

两层自适应超时策略虽然有效地解决了单包流的优化处理问题, 但由于引入了判断误差, 导致流识别的精度有略微降低; 由于没有提出对短流和长流的预先识别机制, 故不能有效地区分短长流, 并采用不同处理机制对其进行优化处理; 由于没有对高层协议相关内容进一步的探讨, 不能支持通过高层协议对网络行为的分析, 这些都是本文未来的研究方向。

## 参考文献

- [1] Claffy K C. Internet traffic characterization. Dissertation for the degree Doctor of Philosophy[D]. University of California, San Diego.1994.
- [2] Claffy K C, H.W.Braun, G.C.Polyzos. A Parameterizable Methodology for Internet Traffic Flow Profiling[J]. In IEEE Journal on Selected Areas In Communications, Vol.12, No.8,Oct. 1995.pages: 1481-1494.
- [3] Ryu B, Cheney D, Braun H.W. Internet Flow Characterization: Adaptive Timeout Strategy and Statistical Modeling[J]. In Workshop on Passive and Active Measurement(PAM), Apr, 2001.
- [4] Jain R, Routhier S A. Packet trains- measurements and a new model for computer network traffic[J]. IEEE JSAC, 4:986-995, 1986.
- [5] Mitchell T.M. Machine Learning[M]. Pressed by China Machine Press. Jan,2003.96-99
- [6] Shaikh A, Rexford J, Shin K.G. Load-Sensitive Routing of Long-lived IP Flows[J]. In Proceedings of SIGCOMM, September 1999.
- [7] Hohn N, Veitch D. Inverting Sampled Traffic[J]. In IMC'03. Oct.2003. Miami Beach, Florida, USA.
- [8] Iannaccone G, Diot C,et al. Monitoring very high speed links[J]. In IMW'01. Nov, 2001. San Francisco, CA, USA.
- [9] Duffield N, Lund C, Thorup M. Properties and Prediction of Flow Statistics from Sampled Packet Streams. In IMW'02. Nov, 2002. Marseille, France.