QoS接纳控制算法的研究与比较*)

高 茜 罗军舟
(东南大学计算机科学与工程系 南京210096)

摘 要 在下一代因特网中,网络服务质量的提供将成为人们关注的热点。要高效、高质量地传输各类业务,就必须通过一个有效的接纳控制机制来保证。本文介绍目前存在的两类QoS接纳控制算法:基于模型的接纳控制算法(Model-Based Connection Admission Control)和基于测量的接纳控制算法(Measurement-Based Connection Admission Control),分析比较了它们的优缺点,并在此基础上提出了一个基于测量的接纳控制算法基本框架。

关键词 QoS,接纳控制,流量模型

Study and Comparison of QoS Admission Control Algorithms

GAO Qian LUO Jun-Zhou
(Department of Computer Science and Engineering,Southeast University,Nanjing 210096)

Abstract In next generation Internet,providing quality of service(QoS)becomes very important. An efficient admission control algorithm is a prerequisite to transmit diverse traffic with high efficiency and quality. This paper describes two kinds of QoS admission control algorithms: Model-Based Connection Admission Control and Measurement-Based Connection Admission Control,and analyzes their prons and cons. Finally a framework of admission control based on measurement is proposed.

Keywords QoS,Admission control,Traffic model

1 引言

在网络技术飞速发展的今天,人们非常关注如何能够高效、高质量地传输各种类型的业务,如多媒体业务。由于网络资源还没有达到用之不竭的程度,所以要高效、高质量地传输各类业务,就必须通过一系列的QoS控制机制来保证,其中包括有效的接纳控制机制[1]。也就是说:接纳一个新流必须同时满足两个条件,一是网络有足够的资源能满足新流所需的QoS,二是接纳该新流以后不会影响已经接纳流的QoS。资源利用率和信元丢失率成为衡量接纳控制算法性能的两个参数。二者是互相矛盾的,网络接纳的流增多了,资源利用率就会提高,然而资源利用率的提高可能导致信元丢失率的增高。所以,一个好的接纳控制算法必须在这两个参数之间做出平衡,使得在满足QoS的前提下有比较高的网络资源利用率。

目前主要有两类接纳控制算法,基于模型的接纳控制算法[3]和基于测量的接纳控制算法[4~10]。基于模型的接纳控制算法要求网络在接纳或拒绝新流的连接请求之前,已经预先知道流量的模型;基于测量的接纳控制算法则无需预知的流量模型,而是通过对网络负载的实施测量来做出接受与否的判断。本文将首先对这两类算法做详细的分析,然后对这两类算法进行比较,并提出了一个基于测量的接纳控制算法基本框架,最后总结全文。

2 基于模型的接纳控制算法

基于模型的接纳控制的实质是在网络做出接纳或拒绝一个新的连接请求的决策之前,通过对流量的模型进行分析,所有相关的参数已经预先求得,所以基于模型的接纳控制算法又称为基于参数的接纳控制算法。由此可见,流量模型的构造在这类算法中尤为重要。

对网络中的业务流的分析及建模不属于本文的研究范畴,在这里,我们主要通过多个独立同分布的业务流聚集在一起时的网络环境来阐明基于模型的接纳控制算法的机理。

2.1 参数估计

当多个独立同分布的业务流量聚集在一起的时候,网络上的流量逐渐成为一个高斯过程[2],而聚集度越高,用高斯过程来描述网络上的流量特性就越准确,所以我们可以利用高斯模型来估计同类聚集流所占用的网络带宽[3]。对于独立的一条连接而言,它所占用的带宽等于流量的均值再加上标准方差的若干倍。其中方差部分是用来满足特殊的QoS需求所需要的特殊带宽。假设k为网络上拥有的连接的数目,C_i为i条连接所占用的带宽,那么当$k=1$时:

$$C_1=\mu+A(1)\sigma \tag{1}$$

其中μ、σ分别为单条流的均值和标准方差。$A(1)$为乘法系数。因此当k条同类业务流聚集在一起时:

$$C_k=\mu k+A(k)(\sigma^2 k)^{1/2} \tag{2}$$

当连接个数k大于一个固定的门槛值时,乘法系数$A(k)$趋于一个固定值,门槛值和乘法系数的确定与缓冲区b的大小有关,并可以通过仿真试验和方程式(2)来确定,我们将试验所得的乘法系数预先存放到一个系数表里,在每次做决策之前,根据k和b来查系数表,再利用(2)式即可计算出具有k

*)本文的研究得到国家973项目"高性能网络协议、算法及软件与系统的研究"课题(G1998030402)与国家自然科学基金会重大研究计划"网络与信息安全"(90204009)的资助。高 茜 博士研究生,主要研究领域为高性能网络协议和算法。罗军舟 博士,教授,博士生导师,主要研究领域为高性能网络、协议工程、分布式系统的建模和性能分析。

条连接并满足 QoS 参数时的网络带宽 C_A。

2.2 决策条件

设 C 为链路总带宽，C_I 为 I 条连接所需要的带宽(包括已经建立的连接和新请求建立的连接)，那么，当：$C_I<C$ 时，新请求的连接被接纳；反之，该连接的请求被拒绝。

3 基于测量的接纳控制算法

与基于模型的接纳控制算法相比，基于测量的接纳控制算法不需要预先知道流量模型，而是通过对网络负载进行实时测量，并以测量出来的结果作为接纳控制的依据。目前基于测量的接纳控制算法很多，但它们主要都由两个部分组成：一是测量算法，二是决策算法，接下来我们就分别介绍一下几种测量算法和决策算法。

3.1 测量算法

3.1.1 *时间窗口测量法* 如图1所示，S 为采样周期，T 为测量窗口，T 为 S 的整数倍。在每个采样周期计算网络的平均负载，在每个测量窗口结束时，我们把各采样周期内最高的负载平均值作为下一个测量窗口的负载估计值；当网络接受一个新流以后，新流的流量就加入到负载估计值值中；如果新计算出来的网络平均负载大于负载估计值，那么就以新计算出来的平均负载作为当前的负载估计值。在每个测量窗口 T 结束之前，网络负载估计值调整到为一个窗口的实际测量值[4]。

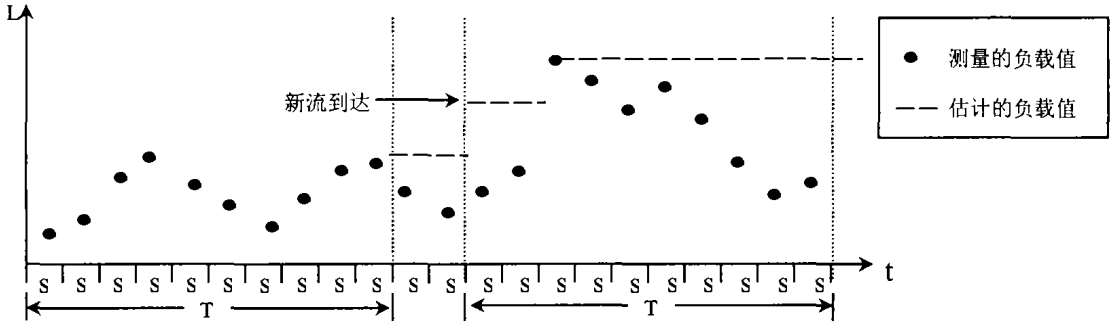

图1 时间窗口测量法

通过调整 S 的大小可以调整测量算法对网络负载变化的敏感程度，S 越大，敏感程度越低，算法越保守；反之，S 越小，敏感程度增大，算法越冒险。T 的大小反映了算法对历史记忆的长度，同样，T 越大，算法越保守，资源利用率越低，接纳流的数目减少；T 越小，通过测量估计所得的负载曲线与网络实际负载曲线拟合的越好，资源利用率越高，但可能导致服务质量的降低。

为了适应网络流量的突发性，文[5,6]提出了自适应的时间窗口测量法。主要原理是根据测得的网络瞬间平均负载，动态调整 S 或 T 的大小来达到自动改进网络接纳能力的目的。

3.1.2 *采样点方法* 以方法(1)中在采样周期 S 里测得的平均负载作为网络负载的估计值。

3.1.3 *指数平均法* 在本方法中，不是估计瞬时带宽，而是估计平均到达速率。在每个 S 结束时测量一次平均到达速率 $\hat{v}'$，那么，我们可以通过一个权重为 w 的无限脉冲响应函数来计算出平均到达速率[7]：

$$\hat{v}'=(1-w)\times\hat{v}+w\times\hat{v}' \tag{3}$$

如果流量的到达速率突然由0变为1并且保持在1，令 $w=2e-3$，那么，10个采样周期后，估计值将达到新速率的75%。

w 越大，算法越能反映出负载的变化。反之，w 越小，平均值越平滑。利用公式(3)也可以计算出一个流的最高速率。设 b 为缓冲区大小，输入流的最高速率为：

$$v^p=\hat{v}'+b/S \tag{4}$$

S 越小，测量的结果越能反映流的突发情况。对最高速率的估计偏差越保守；反之，较大的 S 拥有较长的历史数据记录，平均数值偏低。

3.2 决策算法

3.2.1 *测量和算法* 在本算法中，当新请求的流满足下面这个公式时，新流被接纳，反之，新流的请求被拒绝。

$$\hat{v}+v^p<\mu C \tag{5}$$

其中，$\hat{v}$ 是测量所得的网络负载估计值，v^p 是新流所请求的流量，C 是链路总容量，μ 是用户定义的资源利用率。如文[4]所述，在一个简单的 $M/M/1$ 队列中，如果系统的利用率达到或接近100%，队长的方差将发散，这将使时延变得非常大，进而会导致基于测量的控制算法失败。因此，很有必要定义一个资源利用率目标阈值，例如0.9。使链路利用率低于这个阈值，从而保证控制算法的有效性。

3.2.2 *等价带宽算法* 这种方法利用 Hoeffding bounds 来计算网络上已经建立连接的流的等价带宽。在文[7,11]中 $C(\varepsilon)$ 表示所请求的带宽超过 $C(\varepsilon)$ 的概率为 ε。n 条流基于 Hoeffding bounds 的等价带宽为($\hat{C}_H$)：

$$\hat{C}_H(\hat{v},\{p_i\}\ 1\leqslant i\leqslant n,\varepsilon)=\hat{v}+\sqrt{\frac{\ln(1/\varepsilon)\sum_{i=1}^{n}p_i^2}{2}} \tag{6}$$

其中 $\hat{v}$ 为已建立连接的流的平均到达速率，ε 为到达速率超过链路容量的概率，p_i 为第 i 条流最大到达速率。当一条新流到达时，只要满足 $\hat{C}_H+v^p\leqslant C$，就可以建立连接。

文[8]中介绍了用 Chernoff Bounds 来计算等价带宽的方法，由于篇幅关系，在这里就不一一介绍了。

3.3 相关问题

3.3.1 *历史数据的刷新* 从上面介绍的测量算法我们可以看出，大部分算法得到的都是一段时间内网络负载的平均值，因此算法需要保留一部分历史测量数据，如在基于时间窗口的测量算法中，当前时间窗口 T 内的测量数据都被保留着。如果一条应用流的连接断开，那么它的流量会对测量算法产生什么样的影响呢？显然，对历史数据而言，它的流量依然存在，这就会使网络负载的估计值产生偏差。所以，我们应根据需要对历史数据进行不同程度刷新。

(1)精确刷新。为了对历史数据进行精确刷新，需要将网络上每一条流的测量数据分别存放在一个有限队列里，当其中某条流离开后，测量算法将从该流相应的队列中取出数据，

将其从总的测量流量队列中除去。因此，历史数据中就只包含目前仍然连接着的流的流量。这样便提高了测量算法的准确性，使控制算法的性能大大提高。

然而，这种刷新算法需要对每一条流的流量分别进行测量，并且需要更大的存储空间来保存每条流在每个采样周期内的平均流量。时间复杂度和空间复杂度都增加了 n 倍（n 为连接的数目）。这显然在应用上是不合适的。然而在进行效率和复杂度平衡研究的实验环境中它依然作为一个重要的方法而存在。

(2)粗略刷新。考虑到精确刷新的复杂性，文[9]提出了一种粗略刷新算法，当一个流的连接断开之后，所有的历史数据都减去一个固定的估计值，比如该流的最高速率或平均速率。也就是将离去的流作为一个 CBR 流来对待。显然，这个算法不如算法(1)准确。

3.3.2 *接纳新流之后的反馈* 当接纳一个流之后，网络当前负载应变成新流与网络负载估计值的和，于是，在初始阶段，新流是作为一个 CBR 流来看待的，它的实际流量特性不能全面反映出来，网络就面临着超载的危险。解决这个问题的一个简单方法是，新流的连接建立之后，将网络负载估计得略微偏高一些，或者将3.2.1节中的参数 μ 略微降低一些。

3.3.3 *参数分析* 我们注意到，虽然基于测量的接纳控制算法主要依靠测量所得的结果对新流的连接请求做出判决，有的算法还要求提供该流的一些参数，如：最高到达速率或平均到达速率等。有些算法中的参数可以用来控制接纳算法的性能，如3.2.1节中的资源利用率 μ，μ 增大，则网络资源利用率提高，接纳的流的个数增多。适当的设置参数可以提高算法的性能。

4 两类接纳控制算法的比较

通过前面的研究，我们可以得知基于模型的接纳控制算法的特点是预先需要知道流量模型，算法简单。然而我们也可以从中得出它的缺点：

(1)流量模型不易获得。由于网络上各种应用流到达的随机性，多种流汇聚后的流量特性难以描述，因而难以构造其流量模型。

(2)不能较好地利用网络资源。为了满足 QoS 的要求，常常需要预留资源，基于模型的接纳控制算法通常是以流的最坏情况下所需的资源大小作为预留资源的，这无疑浪费了网络上的宝贵资源。

(3)灵活性比较差。算法大都只适合于某些特定的应用系统，如果将它们运用到互联网上，很多问题就会浮出水面。

与基于模型的接纳控制算法相比，基于测量的接纳控制算法不需要预先知道流量模型，可以在拥有较好的资源利用率的同时满足 QoS 要求，并且通过参数的调整可以控制算法的性能、灵活性比较好。另外，即使流量模型是已知的，一些流（如汇聚的音频流[8]、视频流[12]等）的长程相关性(long-range dependence)，也会对接纳控制产生影响，而基于测量的接纳控制算法可以动态地适应流的长时间范围的波动，从而提高资源利用率。

5 基于测量的接纳控制算法框架

通过前面的分析，我们提出了一个基于测量的接纳控制算法的基本框架。如图2所示，算法的基本步骤如下：

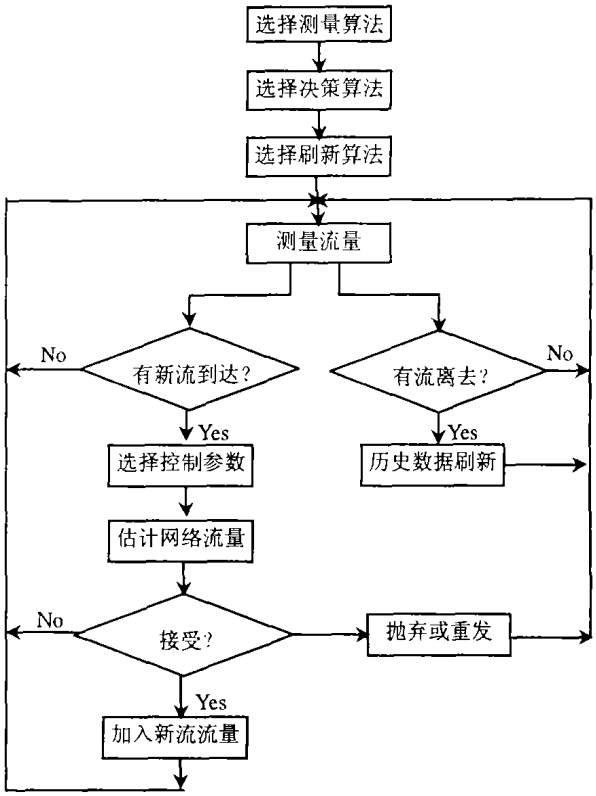

图2 基于测量的接纳控制算法的基本框架

(1)选择合适的测量算法、决策算法以及历史数据刷新算法。

(2)根据测量算法对网络流量进行测量。

(3)如果有新流的连接请求跳到(4)，若有一个流的连接断开跳到(8)。

(4)选择控制参数，估计网络流量。

(5)根据决策算法作出决策，如果新流被接受，跳到(6)，否则跳到(7)。

(6)加入新流的流量到网络流量估计值，若采样时间到返回(2)。

(7)丢弃新流，若采样时间到返回(2)。

(8)根据历史数据刷新算法刷新历史数据，若采样时间到返回(2)。

结束语 接纳控制是网络流量工程的一部分，其目的是在保证一定的服务质量的基础上提高网络资源的利用率。本文介绍了两类接纳控制算法，传统的基于模型的接纳控制算法和基于测量的接纳控制算法，分析了两类算法的基本思想、算法以及其优缺点等，并提出了一个基于测量的接纳控制算法的基本框架。根据这个框架，选择不同的测量算法、决策算法、刷新算法以及控制参数即可得出不同性能的接纳控制算法。

参 考 文 献

1 汪芸，顾冠群. QoS 接入控制必要性研究. 小型微型计算机系统，1999，20(9)

2 Addie B G，Zukerman M，Neame T D. Broadband Traffic Modeling：Simple Soutions to Hard Problems. IEEE Commu-nications Magazine，1998，36：2～9

3 Lee T K，Zukerman M. Practical Approaches for Connection Admission Control in Multiservice Networks. In：Proc. IEEE ICON'99，1999

4 Jamin S，Danzig P B，Shenker S J. A measurement-based Admission Control Algorithm for Integrated Services Packet Networks (Extended Version). ACM/IEEE Transactions on Networking，Dec. 1996

(下转第67页)

信复杂性来讲，本文方案所需消耗的通信量是ITTC方案的$\frac{320(t+1)}{1024(t+1)}\approx 31.2\%$。

另外，在ITTC方案中，系统对M解密的过程中，需要执行t次幂运算$M^{d_i} \bmod N$和$(t-1)$次模数为N的模乘操作，因此，所需的计算总量为：

$$\begin{aligned}240\times t+(t-1) &= 241t-1\text{次} && \text{（模数为 } N \text{ 的模乘操作）}\\ &= (241t-1)41 && \\ &= 9881t-41\text{次} && (F_p \text{ 中域乘操作})\end{aligned}$$

而在本文方案中，通过3.1和4.1节可见，要解密4个长度分别为640比特的密文，系统需要在F_p中完成t次标乘(d_i,y)，$(t-1)$次点加，2次域元求逆和8次域乘操作，因此，需要完成的计算总量为：

$$\begin{aligned}&1200\times t+(t-1)\times(3+2)+2\times 3+8\\ &\quad =1205t+9\text{次} \quad (F_p \text{ 中域乘操作})\end{aligned}$$

由于所选的门限$t\geqslant 1$，显然有$9881t-41>1205t+9$，因此，从计算复杂性来讲，ITTC方案解密所花的时间约为本文方案的$\frac{9881t-41}{1025t+9}\approx 9.64$倍。

因此，我们的方案从效率上比ITTC方案更优。

6.3 可用性

对于一个与Web服务器进行通信的用户而言，Web服务器的私钥以共享的形式存储这一事实对他是透明的。而且，基于(t,n)共享，即使$(n-t)$个共享服务器所存的影子丢失或者服务器因故崩溃，我们的系统也能够提供正常的服务。

所以，本文方案提供了很高的可用性，在可用性方面，本文方案同ITTC方案等价。

7 相关工作

Malkin，Wu和Boneh通过门限RSA方案建立了入侵容忍的Web和CA应用[2]。Fray、Deswarte和Powel在文[9]，以及Deswarte，Blain和Fabre在文[10]中描述了一个加密文件系统，在该系统中，密钥采用Shamir秘密共享方法分别存储在不同的密钥服务器中。当访问一文件时，该文件所对应的密钥需要重建。荆继武、冯登国基于RSA设计了一个入侵容忍CA方案[11]。文[12,13]分别研究了基于ECC的Nyberg-Ruepple门限数字签名方案和ElGamal门限数字签名方案。然而，基于ECC的门限解密方案、基于ECC的入侵容忍应用未见公开的研究发表。

结束语 在本文中，我们提出了一个基于ECC的门限解密方案，设计了一个基于ECC的零知识证明方法，基于提出的方案和方法，对具有入侵容忍功能的Web安全系统进行了研究，并且对我们的方案进行了详细的分析。本文中，我们没有对一些实现细节进行详细描述，下一步我们将完善这些工作。

参考文献

1 Benaloh J C. Secret sharing homomorphisms: keeping shares of a secret secret. In: Proc. Crypto'86. LNCS Vol. 263, Springer

2 Malkin M, Wu T, Boneh D. Building Intrusion Tolerance Applications. In: 8th USENLX Security Symposium

3 Xu Qiuliang, Li Daxing. Elliptic curve cryptosystems[J]. Journal of Computer Research and Development, 1999, 36(11): 1281～1288

4 张险峰，秦志光，刘锦德. 椭圆曲线加密体制的性能分析. 电子科技大学学报，2001，30(2)：144～147

5 朱文余，孙琦. 计算机密码应用基础. 科学出版社，2000. 174～175

6 Frankel Y. A practical protocol for large group oriented network. Eurocrypt 89, pp. 56～61

7 Shamir A. How to Share a Secret. In Communications of the ACM, 1979, 22(11): 612～613

8 Koblitz N, Menezes A, Vanstone S. The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 2000, 19: 173～193

9 Fray J, Deswarte Y, Powell D. Intrusion tolerance using fine-grain fragmentation scattering. In: Proc. IEEE Symposium on Security and Privacy, Oakland, 1986. 194～201

10 Deswarte Y, Blain L, Fabre J. Intrusion tolerance in distributed computing systems. In: Proc. IEEE Symposium on Security and Privacy, Oakland, 1991, 110～121

11 荆继武，冯登国. 一种入侵容忍的CA方案. 软件学报，13(8)

12 Takaragi K, Miyazaki K, Takahashi M, et al. A threshold digital signature issuing scheme without secret communication. http://grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.pdf

13 张险峰，秦志光，刘锦德. 一个基于椭圆曲线的ElGamal型(t,n)门限数字签名方案. 计算机科学，2003，30(5)：157～160

（上接第31页）

5 马小骏，顾冠群. 基于测量的接纳控制研究. 计算机学报，2001，24(1)

6 Lee S, Song J. A Measurement-based Admission Control Algorithm using Variable-sized Window in ATM Networks. In: Intl. Conf. on Information, Communications and Signal Processing, IEEE 1997

7 Floyd S. Comments on Measurement-based Admissions Control for Controlled-Load Services. 1996, URL ftp://ftp.ee.lbl.gov/papers/admit.ps.Z

8 Gibbens R, Keely F. Measurement-Based Connection Admission Control. In: 15th Intl. Teletraffic Congress, Jun. 1997

9 Zukerman M, Tse P W. An adaptive connection admission control scheme for ATM networks. In: Proc. ICC'97, IEEE Intl. Conf. on, Volume: 3, 1997

10 Rhee W, Lee J, et al. Admission control mechanism using measurement based dynamic provisioning in differentiated service networks. In: the 8th Intl. Conf. on Communication Systems, Volume: 1, 2002. 128～132

11 Guerin R, Ahmadi H, Naghshineh M. Equivalent Capacity and Its Application to Bandwidth Allocation in High-Speed Networks. IEEE Journal of Selected Areas in Communication, 1991, 9(7): 968～981

12 Beran J, Sherman R, Taqqu M S, Willinger W. Long-range dependence in variable-bit-rate video traffic. IEEE Transations on Communications, 1995, 43(2)