

分组延迟上限分析策略研究^{*}

郑 瑾¹ 贾维嘉^{1,2}

(中南大学信息科学与工程学院 长沙 410083)¹ (香港城市大学计算机系)²

摘 要 分组延迟上限分析和控制是近年来研究的焦点之一。本文按照分析分组延迟上限所采用策略的不同,对延迟上限的分析策略进行了分类,分析、比较了各类分析策略的特点和优缺点。对未来的研究方向进行了展望,给出了若干值得研究的问题。

关键词 延迟上限,分析策略,保证服务,统计服务

A Survey of Analysis Strategies of Delay Bound

ZHENG Jin¹ JIA Wei-Jia^{1,2}

(School of Information Science and Engineering, Central South University, Changsha 410083)¹

(Department of Computer, Hongkong City University)²

Abstract Much recent year's research has done on finding efficient strategies to analyzes delay bound, This paper categorizes methods of getting worst delay bound, The principle and character of each class of analysis strategy are described and the advantage and disadvantage are discussed. The future directions and some researching problems are also addressed.

Keywords Delay bound, Analysis strategy, Deterministic service, Statistic service

1 引言

近年来,随着 Internet 技术的迅速发展,各种实时应用应运而生,例如视频会议、IP 可视电话、远程医疗、远程实时教育等。这些应用的共同特点是对延迟很敏感。端到端延迟上限的分析在对延迟敏感的服务中非常重要,如果延迟上限太松,则在按延迟要求的接纳控制中,会拒绝一些不该拒绝的服务,从而降低资源利用率。同时如果上限分析结果太乐观,用户被允许接入,将导致网络无法满足其 QoS 延迟保证。另一方面,如果延迟计算太复杂,又会增加处理时间,降低有效性和可扩展性。因此,紧而有效的延迟计算有助于降低接入拒绝率,同时又可提高资源利用率。分组延迟主要包括:传播延迟、传送延迟、处理延迟和排队延迟。传播和传送延迟主要与网络的传输速率和包的大小有关,处理延迟主要取决于调度算法的复杂性。一旦连接建立,传播延迟、传送延迟、处理延迟一般近似不变,因此本文称之为不变延迟,而且容易计算,但排队延迟是可变的,而且要精确地计算出排队延迟是非常困难的,所以很多的延迟分析主要集中在对排队延迟的分析上。排队延迟加上不变延迟,就是端到端的延迟。为了简单起见,本文将排队延迟称之为端到端的延迟。

延迟计算的研究主要集中于两大服务模式:有保障服务和基于概率的(统计)服务。有保障的延迟服务,即用户的连接要求中有一延迟上限要求,如果网络能够满足其延迟上限要求,则允许接入,建立连接,否则网络拒绝该连接请求。对于这类有保障服务,根据延迟上限来决定是否允许接入,一般会造造成拒绝网络本能满足延迟要求的连接请求,从而会降低资源的利用率。对于基于概率的服务模式,即用户提出的延迟上限请求包含概率值,如果网络能在其概率范围内满足其延迟上限,则允许其接入,其代价是偶尔的丢包和超过其延迟上限。但可以提高接入率,从而提高网络资源利用率。

本文在分析延迟上限计算策略的基础上,按照两大服务模式将分析策略采用的方法归纳成几种类型,分析、比较了它们的特点和优缺点,并对未来的研究方向进行了展望。

2 有保障服务中延迟上限分析策略研究进展

2.1 基于分解的分析策略

基于分解的分析策略^[1,2](Decomposed Method)的基本思想是把网络路径分解成一些独立的路由器,依据通信流在本地的属性,算出在每个路由器的排队延迟上限,然后把连接在所要经历的所有路由器上要经历的延迟上限求和,即认为是该流的端到端的延迟上限。其主要优点是:简单并且适合于任何网络拓扑结构下的任何调度算法;主要缺点是:这种端到端的延迟上限的计算未考虑到相继链路的依赖性,而只是简单地通过叠加路径中所有路由器间的延迟的最坏情况来确定延迟上限,这样高估了延迟上限,从而降低了资源利用率。因为一个分组在一个路由器上经历了最坏延迟,却不一定会在其它后继路由器上都会经历最坏延迟,所以这样得到的延迟上限太松,将导致本来网络可满足延迟要求的一些连接请求被拒绝掉。

对于如图 1 所示的一个简单的级连形式的网络拓外结构,该级连结构包括 n 个交换机(路由器),其中有 $2n+1$ 个连接进入网络,连接 0 从第一个交换机的中间端口进入网络,从最后一个交换机的中间端口离开网络,其它连接的流入和流出结构如图 1 所示。

利用分解的方法计算连接 0 在其路径的交换机(路由器)上所经历的延迟上限计算如下:

假设每个进入网络的流都遵循漏桶约束机制,即 $R \sim (a, \rho)$,用 E_k 表示连接 0 在第 k 个交换机(服务器)所经历的延迟上限,则:

$$E_1 = \frac{2a}{1-\rho}; E_2 = a \frac{3-\rho+4\rho^2}{(1-\rho)^2};$$

^{*} 基金项目:国家自然科学基金(60373083)资助。郑 瑾 博士生,主要研究领域为软件工程和计算机网络。贾维嘉 博士,教授,博士生导师,主要研究领域为计算机网络、计算机优化等。

$$E_k = 3a + \rho E_{k-1} + 3\rho \frac{a + \rho \sum_{i=1}^{k-1} E_i}{1 - \rho}, k \geq 3$$

$$D_0^D = \sum_{k=1}^n E_k$$

则连接 0 在整个长度为 n 的路径上的延迟上限为:

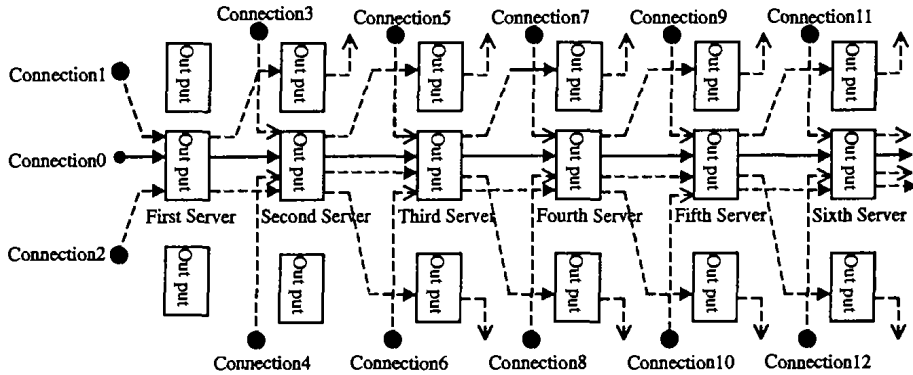


图 1 一个级连结构示意图

2.2 基于集成-分解的分析策略

考虑到基于分解的方法求延迟上限比较简单,但上限太松,Chengzhi Li 等提出一种称为集成-分解的延迟分析方法^[3]。正是由于一个分组在一个路由器上经历最坏延迟,却不一定会在其后继节点一样经历最坏延迟,因此基于分解的方法得到的延迟上限太松。所谓集成-分解的方法,即先将连接所要经历的服务器根据流入流出的次序将服务器分组,算出在每一组内经历的延迟上限和输出流特征,再类似于分解方法,把每一组的延迟上限相加,以此作为端到端的延迟上限。对于图 1 所示的网络拓扑结构,现在需要计算连接 0 在整个长度为 n 的路径上的延迟上限,由于其路径长度为 n ,利用集成-分解的分析策略,按照流入流出的顺序,每两个路由器一组,将其分为 $n/2$ 个组,算出各组的延迟上限,再相加,通过数值计算结果比较,利用这种方法得到的延迟上限比用简单的分解方法得到的上限要紧得多。采用这种分组的方法,可以在一定程度上考虑相继路由器上的延迟相关性,而不是简单机械的相加,所以无论从直观还是从计算结果都表明,这种方法得到的延迟上限要比基于分解的方法得到的上限紧。

但这种方法在计算组内的延迟上限时,由于要考虑相继路由器上的延迟相关性,分析比较复杂,而且只对没有循环的网络结构有效。

2.3 基于服务曲线的分析策略

这其中包括 3 类方法:给连接所经历的服务器分配服务曲线^[4],由调度策略推导服务曲线的方法^[5],基于映射的方法^[6]。

(1) 给连接所经历的服务器分配服务曲线 首先,对连接所经历的路径上的各服务器都指定最小服务曲线,各服务器上的调度策略与最小服务曲线相对应(即调度策略保证满足服务曲线),由这些服务曲线进行卷积运算,算出网络服务曲线(即把具有 n 跳的服务器集合看成一个超级服务器,算出该超级服务器的服务曲线)再根据连接的属性,由此可算出端到端的延迟上限。文[4]描述了调度算法 SCED 匹配基于速率的服务曲线。

理论上这种方法可充分利用网络资源,而且对任意网络拓扑都适用。

缺点:这种方法实现起来太复杂,因为与服务曲线相适应的调度算法总是动态优先算法,调度算法的复杂性也会降低网络资源的利用率。

其分析模型如下:

设一个流 A 的到达曲线为 A^* ,即 $A(t) - A(s) \leq A^*(t - s)$,并且其在某一节点对流 A 的最小服务曲线为 S ,则在该节点所经历的延迟上限计算公式为:

$$d_{\max} = \inf\{d \geq 0 \mid \forall t \geq 0: A^*(t - d) \leq S(t)\} \quad (1)$$

对于要经过多个节点的端到端延迟上限,如图 2 所示。

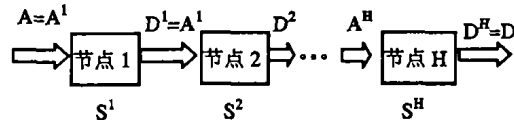


图 2 连接示意图

流 A 经过 H 个节点,其处理办法是将多个服务器集合看成一个超级服务器,由单服务器的服务曲线得到这个超级服务器(网络服务器)的服务曲线,再由上面的单节点的延迟公式计算出端到端延迟上限。设 $S^i (1 < i < H)$ 表示路径上第 i 个服务器的服务曲线, S^{net} 为超级服务器(网络服务器的服务曲线),其计算公式为: $S^{\text{net}} = S^1 * S^2 * \dots * S^H$,其中运算 $*$ 是卷积,其含义是: $(f * g)(t) = \inf_{0 \leq s \leq t} (f(t-s) + g(s))$

因此端到端的计算公式为:

$$d_{\max} = \inf\{d \geq 0 \mid \forall t \geq 0: A^*(t - d) \leq S^{\text{net}}(t)\} \quad (2)$$

由此服务曲线的方法得出的延迟上限非常紧,例如对于保证速率(GR)的调度算法,其计算结果是精确的,但对于其它的调度算法如 FIFO,由于其服务曲线很难精确表达,一般也只能得到近似的服务曲线,因此其结果的精确性难以保证。而且当跳数 H 较大时,由于要进行卷积运算,计算量也很大,实现困难。

(2) 由调度策略推导服务曲线的方法 假设路径上的各个路由器上的调度算法指定,由相应的调度算法推导出各路由器的服务曲线,由此再求出网络服务曲线,再根据通信源的属性,求出端到端的延迟。

优点:这种方法得出的延迟上限较分解的方法要紧。但对于保证速率的调度算法非常紧如对于 GPS 算法。文[5]描述了由调度算法 GPS 推导服务曲线。

缺点:由调度算法推服务曲线很困难,尤其是对于 FIFO 和 SP 调度算法。

(3) 基于映射的方法 将基于多跳的连接映射到只有一个服务器的参照系统下的连接,通常,对于单服务器的连接的延迟分析比较简单,比较原系统和参照系统,通过连接的属性和参照系统的服务器的调度算法,可算出端到端的延迟。文

[6]描述了利用映射计算成本端到端延迟的方法。用这种方法算出的延迟上限比较紧,但是,设计这样的参照系统却不容易。

3 基于概率的延迟上限分析策略研究进展

有保证的网络计算(网络微积分)是计算通信流的延迟保证的有力工具,利用到达曲线和服务曲线^[7],端到端的延迟上限可以用 $\langle \min, + \rangle$ 代数系统精确地表达出来^[7~9]。但是有保证的延迟服务即绝对的延迟保证高估了流实际的资源需求,从而造成了低的网络资源利用率,高估的主要原因在于当有多个流同时竞争网络资源时,在计算延迟上限时,不论是利用分解的方法还是利用服务曲线的方法计算出的延迟上限都是假定多个流同时达到其突发量,但事实上,当流的数量比较大时,大量的流可近似地看成是随机的,各个流同时达到其突发量的概率是比较低的,因此达到最坏延迟的概率也是比较低的,所以,如果是基于延迟有保证的接入控制,就必然会导致本来网络可满足的连接要求被拒绝掉,这样,一方面降低了接入率,另一方面也降低了网络资源的利用率。出于这个考虑,自然就提出了基于概率的延迟服务也称之为统计延迟服务,即在流接入控制阶段,先计算出满足延迟上限的概率,如果在用户的延迟上限概率之内,则允许其接入,这样,一方面可提高接入率,同时又提高网络资源利用率,其代价只是偶尔的丢包和超时。

研究现状:对于基于概率的延迟计算,Kurose^[10]利用随机排序的概念得出了单个流在 FIFO 调度策略下其延迟的概率分布。Chang^[11]提出了到达函数服从指数分布时的延迟的概率上限。对于一些特殊的调度算法,如对于 EDF^[12,13]、GPS^[14]以及其它一些与它们相关的调度算法^[15,16]都已经有一些基于概率的延迟计算结果。为了解决任意网络拓扑结构、任意调度算法的网络结构下概率的延迟计算问题,一些研究人员想到了基于概率的服务曲线,如 Cruz 就定义了概率服务曲线^[17],Chang^[18]提出了对于自适应 F 服务器的基于概率的网络计算方法,Almut Burchard^[19]提出了利用代数系统 $\langle \min, + \rangle$ 来解决基于概率的端到端延迟计算问题,利用 $\langle \min, + \rangle$ 系统来计算端到端延迟,其计算公式的形式非常简单,对于要通过 H 个服务器的连接,其端到端的延迟计算,只要把该路径上的各个节点的有效服务曲线进行卷积运算,求出网络的有效服务曲线,这样,单节点问题就很容易扩充到多节点问题,形式非常简单,其主要思想是提出有效服务曲线的概念,然后借助有保证服务中利用服务曲线计算出延迟上限的方法得到基于概率的端到端的延迟上限。

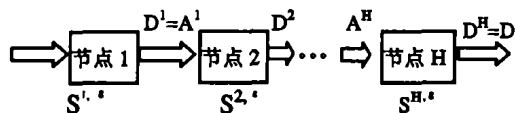


图3 基于概率的连接示意图

对于单节点,若 $\Pr\{D(t) \geq \inf_{x \in [0, T]} \{A(t-x) + S^{\epsilon}(x)\}\}$

T 称为时标, T 要满足不等式 $A^*(T) \leq S^{\epsilon}(T)$, 其中 A^* 表示流 A 的到达曲线, 满足上面概率公式的 S^{ϵ} 称为有效服务曲线, 则其基于概率的延迟上限计算公式为:

$$d_{\max} = \inf\{d \geq 0 \mid \forall t \geq 0 : A^*(t-d) \leq S^{\epsilon}(t)\} \quad (3)$$

而对于要经过多个节点的连接, 其有效服务曲线计算公式:

$$S^{n,\epsilon} = S^{1,\epsilon} * \dots * S^{H,\epsilon} * \delta_{(H-1)\epsilon}$$

$$\text{其中 } \epsilon \leq H\epsilon(1 + (H-1)\frac{T+a}{2a})$$

因此 $\Pr\{D(t) \geq \inf_{x \in [0, H(T+a)]} \{A(t-x) + S^{n,\epsilon}(x)\}\} \geq 1 - \epsilon$

所以过 H 跳的端到端的延迟计算公式为:

$$d_{\max} = \inf\{d \geq 0 \mid \forall t \geq 0 : A^*(t-d) \leq S^{n,\epsilon}(t)\}$$

$$\text{且 } \Pr\{W(t) \leq d_{\max}\} \geq 1 - \epsilon$$

其中, $D(t)$ 是离开过程, 表示 $[0, t]$ 时间段内离开系统的数据量, $W(t)$ 是流在时刻 t 的延迟, a 可取任意正数, 表示在一个服务器经历的固定延迟, 如可以表示流的包化延迟等等, A^* 是流 A 的到达曲线。

从上面的计算公式可以看出, ϵ 与跳数 H 成线性关系, 即当跳数 H 较大时, 满足延迟的概率 $1 - \epsilon$ 就比较小。

这种基于概率的延迟计算方法, 表达形式非常简单, 但也同样存在一些缺陷: 如当跳数 H 很大时, 计算网络的有效服务曲线时, 由于涉及到求卷积, 其计算量很大, 其扩展性不好, 另外, 如何能知道路径上的每个服务器的有效服务曲线, 也是一个难以解决的问题。

4 延迟分析研究趋势

端到端延迟上限分析是服务质量(QoS)的一部分, 同时也是基于延迟的接纳控制研究的一部分, 寻找一种既能得到紧的延迟上限而且有效的简单的延迟计算方法是延迟上限分析研究的主要目标。基于以上的分析, 本文认为未来的研究主要是在提高延迟上限分析方法的有效性、降低延迟计算复杂度、提高可扩展性这三个方面展开。

基于集成-分解的分析方法与简单的分解方法相比, 得到的延迟上限要紧一些, 但目前只是做到每组至多两个服务器, 而且分析很复杂, 是否可扩展到多个服务器为一组即更多地考虑服务器之间延迟的相关性, 在不增加其计算复杂性的基础上, 使计算出的延迟上限更有效即更紧值得进一步研究; 基于服务曲线的延迟上限计算方法虽然形式非常简单, 但由于一方面要求卷积, 计算复杂度高; 另一方面对于不是保证速率的调度算法来说, 得到其精确的服务曲线也是有待进一步研究的问题; 将流数与流量探测以及延迟探测和延迟分析相结合, 得到一种更为紧的有效的基于概率延迟上限的方法是值得进一步研究的方向。在无线网络中, 同样存在延迟保证的问题, 文[20]中提出一种采用流式马尔可夫模型以及有效服务曲线的方法来分析延迟上限, 但分析方法较复杂, 而且当网络系统很大时, 其扩展性不好。所以研究更好的可扩展的无线网络中的概率延迟分析方法, 也是十分必要的。总之, 延迟上限分析在 QoS 中非常重要, 但目前的分析方法在有效性、计算复杂度和可扩展性方面还有许多有待解决的问题。

结束语 随着人们对信息服务需要的日益增长, 对服务质量的要求的一个主要方面是分组延迟上限必须在一定范围之内, 延迟上限分析策略的研究, 对基于延迟上限的接纳控制具有重要意义。本文对现有的延迟分析策略进行了分类和系统分析, 比较了它们的特点和优缺点, 对未来的研究方向进行了展望。

参考文献

1 Cruz R L. A calculus for network delay, Part I: Network elements in isolation. IEEE Transaction of Information Theory, 1991, 37(1): 114~121

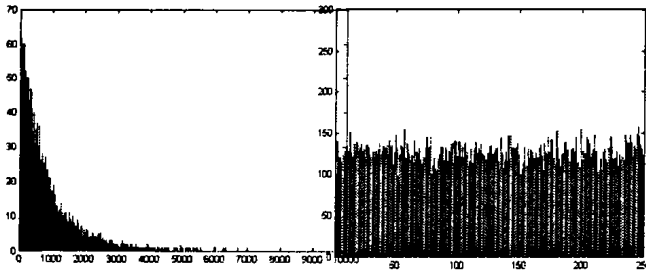


图10 算法二的密文分布

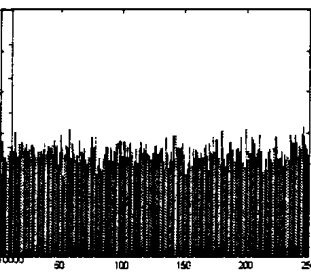


图11 算法三的密文分布

5.4 密钥空间

本文提出算法的密钥长度为64位,如果不考虑混沌系统的结构和参数,那么该算法的密钥空间大小为 2^{64} 。但是算法的64位密钥和混沌系统共同决定S盒的输入序号和加密的轮数,所以密码分析者必须知道S盒的输入序号和加密的轮数以及系统的密钥,在S盒公开的情况下,那么本算法的密钥空间相应增加到 $(2^3)^{32} = 2^{96}$ 。拥有足够大的密钥空间,这对于抵抗穷举攻击具有重要的意义。

5.5 混乱与扩散性能分析

混乱与扩散是设计分组密码的两条基本指导原则。扩散是将每一位明文的影响尽可能地作用到较多的输出密文位中去,同时,还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的密文位中去。其目的是有效隐藏明文的统计特性,这也就是混沌系统的初始条件敏感依赖性。混乱,是指密文和明文之间的统计特性的关系尽可能的复杂化,这也就是混沌映射通过迭代,将初始域扩散到整个相空间。通过混沌和扩散,可以有效地抵抗统计和抗差分攻击。

在传统分组密码算法中,其置乱都是基于预先编排好置换盒(如DES的P盒),它只是重新编排了明文分组排序而已,对加密过程中所要求的混乱和扩散特性的贡献非常小,以至于在差分分析和线性密码分析中都将其效果忽略不计。而在本文所提算法中,加密的轮次和子密钥决定明文分组置乱效果,而加密的轮次和子密钥是基于混沌系统动态更新的,即混沌

系统的初始值和控制参数是紧密相关的,所以这种置乱是敏感地依赖于密钥且随机的,大大增加了密码系统的混乱与扩散特性。

结论 本文较详细地分析了Hénon映射的混沌特性和密码学特性,并根据这些特点,设计出一种新颖的基于Hénon映射和Feistel结构的分组密码算法,该算法不同于传统分组密码算法(如DES,HOST等)的最大特点是:加密的轮数盒子密钥的生成基于混沌系统动态更新的。同时,混沌系统的本质特性使得算法的复杂度极大地提高,从而更难以分析和预测。实验结果同时也表明并从理论上证明了其具有较强的抵抗差分密码分析和线性密码分析的能力和较高的安全性。

参考文献

- 1 Matthews R. On the derivation of a chaotic encryption algorithm. *Cryptologia*, XIII (1), 1989. 29~42
- 2 Habutsu T, Nishio Y, Sasase I, et al. A secret cryptosystem by iterating a chaotic map. *Advance in cryptology - EUROCRYPT'91*, LNCS 547 (Springer - Verlag, Berlin), 1991. 127~140
- 3 Biham E. Cryptanalysis of the chaotic-map cryptosystem suggested as EUROCRYPT'91. *Advance in cryptology - EUROCRYPT'91*, LNCS 547 (Springer - Verlag, Berlin), 1991. 532~534
- 4 Kocarev L, Jakimoski G. Logistic map as a block encryption algorithm. *Phys. Lett. A*, 2001, 289(4-5): 199~206
- 5 Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table. *Phys. Lett. A*, 2002, 298(4): 238~242
- 6 Jakimoski G, Kocarev L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. *IEEE Trans. on circuits and systems-I*, 2001, 48(2)
- 7 Jridich J. Image Encryption Based on Chaotic Maps. *Systems, Man and Cybernetic*, 1997, 'Computational Cybernetics and Simulation', 1997 IEEE Intl. Conf. on, 1997, 2
- 8 吴世忠,等译. 应用密码学. 机械工业出版社, 2000
- 9 Erdmann D, Murphy S. Henon Stream Cipher. *Electronics Letters* 23rd, April 1992, 28(9)
- 10 Feistel H. Cryptography and computer privacy. *Scientific American*, 1973, 5: 15~23
- 11 Feistel H. Stemp Code Ciphering System. U. S. Patent, 1974, 3: 359~400

(上接第28页)

- 2 Cruz R L. A calculus for network delay, Part II: Network analysis. *IEEE Transactions on Information Theory*, 1991, 37(1): 132~141
- 3 Li C, Bettati R, Zhao W. New Dealy Analysis in High Speed Networks
- 4 Cruz R L. Quality of service guarantees in virtual circuit switched networks. *IEEE journal on Selected Areas in communications*. 1995, 13(6): 1048~1056
- 5 Parekh A K J. A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks. [Ph. D. dissertation]. Massachusetts Institute of Technology. Cambridge, MA, 1992
- 6 Figueira N R, Pasquale J. An upper bound on delay for the virtual clock service discipline. *IEEE/ACM Transactions on Networking*, 1995, 3(4): 399~408
- 7 Agrawal R, Cruz R L, Okino C, Rajan R. Performance bounds for flow control protocols. *IEEE/ACM Transactions on Networking*, 1999, 7(3): 310~323
- 8 Boudec J Y L. Application of network calculus to guaranteed service networks. *IEEE/ACM Transactions on Information Theory*, 1998, 44(3): 1087~109
- 9 Chang C S. On deterministic traffic regulation and service guarantees: a systematic approach by filtering. *IEEE/ACM Transactions on Information Theory*, 1998, 44(3): 1097~1110
- 10 Kurose J. On computing per-session performance bounds in high-speed multi-hop computer networks. In *ACM Sigmetrics'92*, 1992. 128~139
- 11 Chang C S. Stability, queue length, and delay of deterministic and

- stochastic queueing networks. *IEEE Transactions on Automatic Control*, 1994, 39(5): 913~931
- 12 Sivaraman V, Chiussi F M. Statistical analysis of delay bound violations at an earliest deadline first scheduler. *Performance Evaluation*, 1999, 36(1): 457~470
- 13 Sivaraman V, Chiussi F M. Providing end-to-end statistical delay guarantees with earliest deadline first scheduling and per-hop traffic shaping. In: *Proc. of IEEE Infocom 2000*, Tel Aviv, March 2000. 603~612
- 14 Elwalid A, Mitra D. Design of generalized processor sharing schedulers which statistically multiplex heterogeneous QoS classes. In: *Proc. of IEEE INFOCOM'99*, New York, March 1999. 1220~1230
- 15 Andrews M. Probabilistic end-to-end delay bounds for earliest deadline first scheduling. In: *Proc. of IEEE Infocom 2000*, Tel Aviv, March 2000. 603~612
- 16 Li C, Knightly E. Coordinated network scheduling: A framework for end-to-end services. In: *Proc. of IEEE ICNP 2000*, Osaka, Nov. 2000
- 17 Cruz R L. Quality of service management in integrated services networks. In: *Proc. of the 1st Semi-Annual Research Review*, CWC, UCSD, June 196
- 18 Chang C S. *Performance Guarantees in Communication Networks*. Springer Verlag, 2000
- 19 Burchard A, Liebeherr J, Patek S. A Calculus for End-to-end Statistical Service Guarantees. [Technical Report; CS-2001-19]. 2001
- 20 Wang S, Nathuji R, Bettati R, Zhao W. Providing Statistical Guarantees in Wireless Networks. In: *Proc. of the IEEE Intl. Conf. on Distributed Computing Systems (ICDCS 2004)*, March 2004