文章编号: 1001-0920(2006)11-1239-05

动态Internet拥塞控制算法

杨洪勇[1,2], 张福增[1], 王福生[1], 张嗣瀛[2]
(1. 鲁东大学 计算机学院, 山东 烟台 264025; 2. 东北大学 信息科学与工程学院, 沈阳 110004)

摘 要: 基于网络优化原理, 建立了一个在网络的源节点和连接节点都是动态变化的Internet拥塞控制算法. 通过讨论具有通信时延的动态Internet拥塞控制算法的频率曲线, 得到了时滞函数的许多频域特性; 应用多变量频域控制理论, 分析了时延不同的动态Internet拥塞控制算法在平衡点的渐近稳定性. 最后, 通过仿真验证了结论的有效性.

关键词: Internet; 动态拥塞控制算法; 通信时延; 渐近稳定性;
中图分类号: TP393 **文献标识码**: A

Dynamic Congestion Control Algorithm for the Internet

YANG Hong-yong[1,2], *ZHANG Fu-zeng*[1], *WANG Fu-sheng*[1], *ZHANG Si-ying*[2]
(1. School of Computer Science and Technology, Ludong University, Yantai 264025, China; 2. College of Information Science and Engineering, Northeastern University, Shenyang 110004, China. Correspondent: YANG Hong-yong, E-mail: hyyang@yeah.net)

Abstract: Based on the optimality principle of the network, a dynamic Internet congestion control algorithm (DICCA) at the resources and the link nodes is presented. Some frequency characteristics are obtained by discussing the frequency plots of the DICCA with communication delays. By using multi-variable frequency control theories, the asymptotical stabilities of the algorithm at the equilibrium point are analyzed. Finally, computer simulations show the validity of these results.

Key words: Internet; Dynamic congestion control algorithm; Communication delay; Asymptotical stability

1 引 言

Internet的拥塞控制问题受到了越来越多的关注, 现在Internet的流量控制是基于Jacobon提出的拥塞窗口控制算法[1]改进得到的TCP Reno, 中间节点的主动队列管理策略采用Floyd等提出的RED控制算法[2]. 但是近期的研究表明RED算法对网络的参数设置和运行状况比较敏感, 会引起节点队列大幅振荡、吞吐量降低、时延增加等网络不稳定现象[3,4]. 为了最大限度提高网络的利用率, 保证网络的稳定性能, 许多文献提出了改进的网络拥塞控制算法: ARED[5], Kelly算法[6], REM[7]等.

在确定一个新的网络拥塞控制算法是否可行之前, 必须事先对该算法从理论上进行分析, 研究这些算法的性能以及稳定性等问题. 假设在将来, 随着网络线路上硬件和网络能力的提高, 队列时延会逐渐减少, 与传播时延相比非常小, 从而在网络通信时延中可以只考察传播时延, 忽略队列时延[8,9]. 在该假设下, 文献[10]研究了[6]提出的主算法的稳定性, 得到各源节点具有相同通信时延时的系统局部稳定的充分条件. 假设各源节点具有不同的通信时延, 文献[10]给出了系统在平衡点局部渐近稳定的一个猜想. 文献[11~13]分别研究了该猜想, 最后文献[11]给出了一个比猜想更强的结论, 同时也证明了猜想的正确性.

在实际的Internet网络系统中源节点采用动态的TCP Reno算法来调整发送窗口大小; 连接节点采用AQM策略(如RED等)来动态调整节点的分组标识率. 也就是说, 源节点和连接节点的拥塞控制算

收稿日期: 2005-09-21; **修回日期**: 2006-02-23.
基金项目: 国家自然科学基金项目(60574007); 鲁东大学校基金项目(22320301).
作者简介: 杨洪勇(1967—), 男, 山东庆云人, 教授, 博士后, 从事非线性控制、鲁棒控制等研究; 张嗣瀛(1925—), 男, 山东章丘人, 中国科学院院士, 教授, 博士生导师, 从事复杂系统的相似结构与全息性质等研究.

法都是动态的. 本文从实际网络背景出发, 根据最优控制原理, 建立一个新的动态 Internet 拥塞控制算法: 源节点的速率和连接节点的拥塞概率通过不同的拥塞控制算法进行动态调整. 需要说明的是: 本文构建的拥塞控制算法与文献[6]给出的拥塞控制算法不同, 文献[6]建立的主算法中源节点的速率是根据一个非线性方程动态调整, 而连接节点的拥塞率采用一个静态函数来调整; 文献[6]的对偶算法中的拥塞概率采用一个动态方程调整, 源节点速率则采用一个静态函数来确定.

2 动态 Internet 拥塞控制算法

2.1 动态 Internet 拥塞控制的算法模型

考虑多源节点和多连接节点的网络通信系统. 连接点集合 $L = \{1, \cdots, L_0\}$, 源节点集合 $N = \{1, \cdots, N_0\}$. 在网络中一个源节点可以与多个连接节点连接; 反过来, 每个连接节点可以有多个源节点共享. 对于每一个连接节点 l, 设 p_l 和 c_l 分别为连接节点的连接价格(拥塞概率) 和连接能力, 使用连接节点 l 的源节点集合为 $N(l) \in N$, 所有使用 l 的源节点传输率之和(网络负载) 为 y_l. 对于每一个源节点 $i \in N$, 设源节点速率为 x_i, 源节点 i 使用的连接节点集合为 $L(i) \in L$, 源节点 i 使用的所有连接节点的总拥塞率为 q_i. 定义 $L_0 \times N_0$ 维的路由矩阵 $R = (R_{li})_{L_0 \times N_0}$ 为

$$R_{li} = \begin{cases} 1, & l \in N(l); \\ 0, & \text{其他} \end{cases}$$

本文中假定路由矩阵 R 是行满秩的, 即只考虑网络系统中的瓶颈连接.

根据以上假设, 得到下面的公式:

$$\begin{aligned} y(t) &= Rx(t), \\ q(t) &= R^{\mathrm{T}} p(t). \end{aligned} \tag{1}$$

式中: R^{T} 表示矩阵 R 的转置, 向量 $y(t) = (y_1(t), \cdots, y_{L_0}(t))^{\mathrm{T}}$, $x(t) = (x_1(t), \cdots, x_{N_0}(t))^{\mathrm{T}}$, $q(t) = (q_1(t), \cdots, q_{N_0}(t))^{\mathrm{T}}$, $p(t) = (p_1(t), \cdots, p_{L_0}(t))^{\mathrm{T}}$.

假设网络系统中每一个源节点都有一个效益函数 $u_i(x_i(t))$ (该函数是关于速率 x_i 递增的、光滑的严格凹函数), 那么构成一个网络系统最优化问题: 对于所有的 $x \geq 0$,

$$\max_x U(x), \quad \text{s.t.} \quad y \leq c$$

这里: $U(x) = \sum_{i \in N} u_i(x_i(t))$ 为网络系统的总效益函数, $c = (c_l, l \in L)$ 为连接节点的服务能力[6]. 本文建立一个 Lagrange 函数, 把系统有约束的最优化问题化为无约束优化问题, 即

$$L(x, p) = \sum_{i \in N} u_i(x_i) + \sum_{l \in L} p_l(c_l - y_l). \tag{2}$$

其中拥塞率 p_l 称为 Lagrange 乘子. 根据式(1), 式(2) 可变为

$$L(x, p) = \sum_{i \in N} (u_i(x_i) - x_i q_i) + \sum_{l \in L} p_l c_l. \tag{3}$$

根据最优控制原理, 本文建立一个新的 Internet 拥塞控制算法, 源节点和连接节点的拥塞控制算法都是动态的. 令

$$\dot{x}_i(t) = k_i \frac{\partial L(x, p)}{\partial x_i}, \quad \dot{p}_l = -k_l \frac{\partial L(x, p)}{\partial p_l},$$

则有

$$\begin{aligned} \dot{x}_i(t) &= k_i(u_i'(x_i) - q_i(t)), \\ \dot{p}_l &= k_l(y_l - c_l). \end{aligned} \tag{4}$$

可以看到, 拥塞控制算法(4) 具有如下运行特性: 源节点的速率的动态调整只与该节点接收到的来自连接节点的总拥塞率有关, 与其他源节点信息无关; 连接节点 l 的拥塞率的动态调整只与该节点的网络负载有关, 与其他连接节点信息无关. 假设系统(4) 存在平衡点 (x_i^*, p_l^*), 易知平衡点满足

$$\begin{aligned} x_i^* &= u_i'^{-1}(q_i^*), \\ y_l^* &= c_l. \end{aligned} \tag{5}$$

这里: $q_i^* = \sum_{l \in L(i)} p_l^*$ 为系统平衡时对应的总连接价格, $y_l^* = \sum_{i \in N(l)} x_i^*$ 为系统的平衡负载.

2.2 时延微分方程的线性化

假设 $d_1(l, i)$ 是数据由源节点 i 传输到连接节点 l 的时延, $d_2(l, i)$ 是反馈信号由连接节点 l 到达源节点 i 的时延. 这样在通信网络系统中每一个回路对应一个往返时延, 记 D_i, 显然 $d_1(l, i) + d_2(l, i) = D_i$, $i \in N$. 则式(1) 变为

$$\begin{aligned} y(t) &= Rx(t - d_1(l, i)), \\ q(t) &= R^{\mathrm{T}} p(t - d_2(l, r)). \end{aligned}$$

Laplace 变换后假设

$$R(s) = R(\mathrm{e}^{-sd_1(l, i)}) = (R_{li}\mathrm{e}^{-sd_1(l, i)}),$$

则有

$$\begin{aligned} y(s) &= R(s)x(s), \\ q(s) &= \mathrm{diag}(\mathrm{e}^{-sD_i}) R^{\mathrm{T}}(-s) p(s). \end{aligned} \tag{6}$$

在平衡点附近, 假设

$$\begin{aligned} p_l(t) &= p_l^* + \hat{p}_l(t), \\ x_i(t) &= x_i^* + \hat{x}_i(t), \end{aligned}$$

相应地有

$$y_l(t) = y_l^* + \hat{y}_l(t), \quad q_i(t) = q_i^* + \hat{q}_i(t).$$

这里: $\hat{p}_l(t), \hat{y}_l(t), \hat{q}_i(t), \hat{x}_i(t)$ 为系统在平衡点的干扰量. 把方程(4) 进行线性化, 忽略高阶无穷小项, 得

$$\begin{aligned} \dot{\hat{x}}_i(t) &= k_i(u_i'' \hat{x}_i(t) - \hat{q}_i(t)), \\ \dot{\hat{p}}_l(t) &= k_l \hat{y}_l \end{aligned}$$

这里 $u_i'' < 0$ 表示效益函数在平衡点处的二阶导数. 对上式作 Laplace 变换, 整理得到速率到速率的闭环系统为

$$x(s) = \mathrm{diag}\left(\frac{-k_i}{s - k_i u_i''}\frac{\mathrm{e}^{-sD_i}}{s}\right) R^{\mathrm{T}}(-s) K R(s) x(s), \tag{7}$$

这里 $K = \mathrm{diag}(k_l, l \in L)$, 那么系统的开环传递函数

$$G(s) = \mathrm{diag}\left(\frac{-k_i}{s - k_i u_i''}\frac{\mathrm{e}^{-sD_i}}{s}\right) R^{\mathrm{T}}(-s) K R(s), \tag{8}$$

设系统开环传递函数(8) 中右边对角矩阵的矩阵元素变形为

$$H(x) = \frac{A}{\mathrm{j}x + A}\frac{\mathrm{e}^{-\mathrm{j}x}}{\mathrm{j}x}, \quad A > 0.$$

下面研究函数 $H(x)$ 的频率特性.

3　函数 H(x) 的 Nyquist 曲线特性

引理 1　$H(x)$ 的 Nyquist 曲线是顺时针的.

证明略.

由于 $H(x) = H^*(-x)$ 函数关于实轴对称, 因此只需考察 $x \in (0, +\infty)$ 时的 $H(x)$ 的 Nyquist 曲线特性.

引理 2　假设 $x = x_0$ 时 $H(x)$ 的 Nyquist 曲线与实数轴第一次相交, 则 x_0 是 A 的增函数.

证明略.

由于 $|H(x)| = A/(x\sqrt{x^2 + A^2})$ 是 x 的减函数, 又由于 $H(x)$ 的 Nyquist 曲线是顺时针的, 采用与文献[11] 中的 Proposition 3 类似的证明过程, 可以得到:

引理 3　假设 $x = x_0$ 时 $H(x)$ 的 Nyquist 曲线与实数轴第一次相交, $H(x)$ 的 Nyquist 曲线都位于过该点的切线 $r(x_0)$ 右边(包含切点).

引理 4　假设 $x = x_0$ 时 $H(x)$ 的 Nyquist 曲线与实数轴第一次相交, 过该点的切线 $r(x_0)$ 的斜率为 $T(x_0)$, 则 $T(x_0)$ 是 A 的增函数.

引理 5　假设在 $x \in (0, +\infty)$ 内, $H_i(x) = \frac{A_i}{\mathrm{j}x + A_i}\frac{\mathrm{e}^{-\mathrm{j}x}}{\mathrm{j}x}$ 的 Nyquist 曲线第一次交实轴于 $x = x_i$, 其中 $i = 1, 2$ 则对于任意的 $b_i < 1/|H(x_i)|$, 有 $(-1, \mathrm{j}0) \notin \mathrm{Co}(b_1 H_1(x), b_2 H_2(x))$. $\mathrm{Co}(\bullet)$ 表示集合的凸包.

证明　根据题设可知: 对于 $b_i < 1/|H(x_i)|$, $i = 1, 2$, 有 $(-1, \mathrm{j}0)$ 在 $b_i H_i(x)$ 与实轴交点的左边. $b_1 H_1(x)$ 的 Nyquist 曲线与 $b_2 H_2(x)$ 的 Nyquist 曲线的第一个交点有下列 3 种情况: 1) 交点在实轴上; 2) 交点在实轴下方; 3) 交点在实轴上方. 本文只证明第 1) 种情况. 不妨假设 $A_1 < A_2$, 根据引理 2 可以知道 $x_1 < x_2$. 下面讨论 x 分别在区间 $(0, x_1)$, $[x_1, x_2]$ 和 $(x_2, +\infty)$ 内的 3 种情况.

1) 当 $x \in (0, x_1)$ 时, 函数还没有到达与实轴第一次相交的临界点, 此时 $b_i H_i(x)$ 的 Nyquist 曲线都在第三象限, 由于 $(-1, \mathrm{j}0)$ 在 $b_i H_i(\omega)$ 与实轴交点的左边, 引理结论正确.

2) 当 $x \in [x_1, x_2]$ 时, 此时 $b_2 H_2(x)$ 的 Nyquist 曲线在实轴下方, $b_1 H_1(x)$ 的 Nyquist 曲线在实轴上方. 根据引理 3 可知, $b_i H_i(x)$ 的 Nyquist 曲线分别位于自己临界点处切线 $r(x_i)$ 的右边(包含切点). 当 $A_1 < A_2$ 时, 由引理 4 可知在临界点处切线的斜率满足: $T(x_1) < T(x_2)$, $b_2 H_2(x)$ 的 Nyquist 曲线位于切线 $r(x_2)$ 下半部分的右边, $b_1 H_1(x)$ 的 Nyquist 曲线位于切线 $r(x_1)$ 上半部分的右边. 也就是凸包 $\mathrm{Co}(b_1 H_1(x), b_2 H_2(x))$ 位于切线 $r(x_2)$ 和 $r(x_1)$ 右边区域的交集中, 如图 1 所示. 其中: 直线 R 表示切线 $r(x_2)$; 直线 r 表示切线 $r(x_1)$. 由于 $(-1, \mathrm{j}0)$ 在 $b_i H_i(x)$ 与实轴交点的左边, 所以有 $(-1, \mathrm{j}0) \notin \mathrm{Co}(b_1 H_1(x), b_2 H_2(x))$.

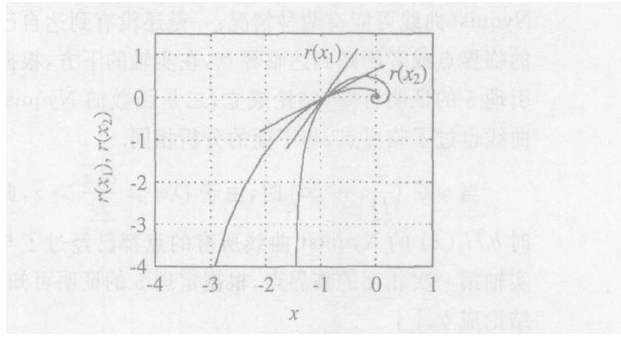

图 1　$b_i H_i(x)$ 的 Nyquist 曲线及在临界点处的切线

3) 当 $x \in (x_2, +\infty)$ 时, 函数都过了与实轴第一次相交的临界点, 由引理 4 可知当 $A_1 < A_2$ 时, 有 $T(x_1) < T(x_2)$, 所以 $b_1 H_1(x)$ 的 Nyquist 曲线位于 $b_2 H_2(x)$ 的 Nyquist 曲线的右边. 由于 $|b_2 H_2(x)| < 1$ 且 $|b_2 H_2(x)|$ 随着 x 增大逐渐减小, 所以 $b_2 H_2(x)$ 的 Nyquist 曲线没有自相交. 由于 $(-1, \mathrm{j}0)$ 在 $b_2 H_2(x)$ 与实轴交点的左边, 有 $(-1, \mathrm{j}0) \notin \mathrm{Co}(b_1 H_1(x), b_2 H_2(x))$. 结论正确.

采用相类似的证明方法, 可得到后两种情况的结论也是正确的. □

推论 1　假设

$$H_i(x) = \frac{A_i}{\mathrm{j}x + A_i}\frac{\mathrm{e}^{-\mathrm{j}x}}{\mathrm{j}x}, \quad i = 1, 2$$

的 Nyquist 曲线第一次交实轴于 $x = x_i$. 设 $x = D_i\omega$, $A_i = D_i\alpha_i$, 则对于任意的 $b_i < 1/|H(x_i)|$, 有

$$(-1, \mathrm{j}0) \notin \mathrm{Co}(b_1 H_1(\omega), b_2 H_2(\omega)).$$

这里: $H_i(\omega) := H_i(D_i\omega)$, $\mathrm{Co}(\bullet)$ 表示集合的凸包.

证明 记 $\overline{x} = \max_{i=1,2}(x_i)$, $\underline{x} = \min_{i=1,2}(x_i)$, $\overline{D} = \max_{i=1,2}(D_i)$, $\underline{D} = \min_{i=1,2}(D_i)$. 根据题意可知当 $\omega = x_i/D_i$ 时, $H_i(D_i\omega)$ 的Nyquist曲线与实轴第一次相交. 采用和引理5相类似的证明方法, 讨论 ω 分别属于区间 $\left(0, \frac{\underline{x}}{\overline{D}}\right)$, $\left[\frac{\underline{x}}{\overline{D}}, \frac{\overline{x}}{\underline{D}}\right]$ 和 $\left(\frac{\overline{x}}{\underline{D}}, +\infty\right]$ 内的3种情况.

当 $\omega \in \left(0, \frac{\underline{x}}{\overline{D}}\right)$ 时, 由于 $D_i\omega < \frac{D_i\underline{x}}{\overline{D}} \leq \underline{x}$, 函数 $b_iH_i(x)$ 的Nyquist曲线没有到达与实轴第一次相交的临界点, 曲线上的所有点都在第三象限, 所以有 $(-1, j0) \notin \mathrm{Co}(b_1H_1(\omega), b_2H_2(\omega))$, 这样推论成立.

当 $\omega \in \left[\frac{\underline{x}}{\overline{D}}, \frac{\overline{x}}{\underline{D}}\right]$ 时, 因为

$$\omega = \frac{x_i}{D_i} \geq \frac{\underline{x}}{D_i} \geq \frac{\underline{x}}{\overline{D}},\quad \omega = \frac{x_i}{D_i} \leq \frac{\overline{x}}{D_i} \leq \frac{\overline{x}}{\underline{D}},$$

临界频率都在区间 $\left[\frac{\underline{x}}{\overline{D}}, \frac{\overline{x}}{\underline{D}}\right]$ 内, 频率在该区间变化时, 最快的 $b_iH_i(x)$ 的Nyquist曲线经过了与实轴第一次相交的临界点, 在实轴的上方. 慢的 $b_iH_i(x)$ 的Nyquist曲线可能有两种情况: 一是还没有到达自己的临界点或者刚好到达临界点, 在实轴的下方, 根据引理5的证明可知, 结论成立; 二是函数的Nyquist曲线也过了临界点, 与下面的分析相同.

当 $\omega \in \left(\frac{\overline{x}}{\underline{D}}, +\infty\right)$ 时, 由于 $D_i\omega \geq \frac{D_i\overline{x}}{\underline{D}} > \overline{x}$, 此时 $b_iH_i(x)$ 的Nyquist曲线所有的点都已经过了与实轴第一次相交的临界点, 根据定理5的证明可知, 结论成立. □

4 具有通信时延的拥塞控制算法的稳定性

开环传递函数(8)中令 $s = j\omega$, 可以得到

$$G(j\omega) = \mathrm{diag}\left(\frac{k_i}{j\omega - k_iu_i''}\frac{e^{-j\omega D_i}}{j\omega}\right)R^{\mathrm{T}}(-j\omega)KR(j\omega).$$

定理1 对于任意的 $i \in N$, 设 $x = D_i\omega$, $A_i = D_i\alpha_i$, $\alpha_i = -k_iu_i''$, 在 $x \in (0, +\infty)$ 内, 当 $x = x_i$ 时 $H_i(x) = \frac{A_i}{jx + A_i}\frac{e^{-jx}}{jx}$ 的Nyquist曲线与实轴第一次相交. 则当 $b_i < 1/|H(\omega)|$ 时, 系统在平衡点是局部渐近稳定的. 这里 $b_i = -\left(D_i\sum_{l\in L}R_{li}K_l\sum_{r\in N}R_{lr}\right)/u_i''$, $u_i'' < 0$ 表示效益函数在平衡点处的二阶导数, $H_i(\omega) = H(D_i\omega)$, $\omega = x_i/D_i$.

证明 根据前面的讨论, 由引理3可知 $H_i(\omega)$ 的Nyquist曲线是顺时针的, 曲线都在临界点切线的右边, 当然原点也在切线的右边, 所以有

$$\mathrm{Co}(0, \{b_iH_i(\omega), i = 1, \cdots, N_0\}) = \mathrm{Co}(b_iH_i(\omega), i = 1, \cdots, N_0).$$

由推论1可得 $(-1, j0) \notin \mathrm{Co}(0, \{b_iH_i(\omega), i = 1, \cdots, N_0\})$.

对式(8)进行简单变换, 可得

$$G(j\omega) = \mathrm{diag}(b_iH_i(\omega), i = 1, \cdots, N_0)\hat{R}^{\mathrm{T}}(-j\omega)\hat{R}(j\omega).$$

这里

$$\hat{R}^{\mathrm{T}}(-j\omega) = \mathrm{diag}\left(\sqrt{-\frac{D_i}{b_iu_i''}}\right)R^{\mathrm{T}}(-j\omega)\mathrm{diag}(\sqrt{\kappa_l}).$$

由于

$$\rho(\hat{R}^{\mathrm{T}}(-j\omega)\hat{R}(j\omega)) = \rho\left(\mathrm{diag}\left(\sqrt{-\frac{D_i}{b_iu_i''}}\right)R^{\mathrm{T}}(-j\omega)KR(j\omega)\mathrm{diag}\left(\sqrt{-\frac{D_i}{b_iu_i''}}\right)\right) = \rho\left(\mathrm{diag}\left(-\frac{D_i}{b_iu_i''}\right)R^{\mathrm{T}}(-j\omega)\mathrm{diag}(\kappa_l, l \in L)R(j\omega)\right) \leq \max_{i\in N}\left(-\frac{D_i}{b_iu_i''}\sum_{l\in L}R_{li}\kappa_l\sum_{r\in N}R_{lr}\right) = 1.$$

这里 $\rho(\cdot)$ 表示矩阵的谱半径. 设 λ 为矩阵 $G(j\omega)$ 的特征值, 则存在向量 v, $\|v\| = 1$, 满足

$$\hat{R}(j\omega)\mathrm{diag}(b_iH_i(\omega))\hat{R}^{\mathrm{T}}(-j\omega)v = \lambda v,$$

则有

$$\lambda = v^*\hat{R}(j\omega)\mathrm{diag}(b_iH_i(\omega), i \in N)\hat{R}^{\mathrm{T}}(-j\omega)v,$$

这里 v^* 表示向量 v 的共轭转置. 由于

$$\|\hat{R}^{\mathrm{T}}(-j\omega)v\| = \rho(\hat{R}^{\mathrm{T}}(-j\omega)\hat{R}(j\omega)) \leq 1,$$

可得

$$\lambda \in \mathrm{Co}(0, \{b_iH_i(\omega), i = 1, \cdots, N_0\}).$$

由于

$$(-1, j0) \notin \mathrm{Co}(0, \{b_iH_i(\omega), i = 1, \cdots, N_0\}),$$

根据广义Nyquist判据得到系统在平衡点是局部渐近稳定的. □

推论2 假设时延系统(4)的平衡点是 (p^*, x^*), 系统在平衡点局部渐近稳定的充分条件为

$$-\left(D_i\sum_{l\in L}R_{li}\kappa_l\sum_{r\in N}R_{lr}\right)/u_i'' < 1,\quad i = 1, \cdots, N_0,$$

这里 u_i'' 为效益函数在平衡点的二阶导数值.

证明 因函数 $b_iH_i(\omega)$ 的Nyquist曲线在临界点满足

$$D_i\omega + \mathrm{arctg}\left(\frac{\omega}{\alpha_i}\right) = \frac{\pi}{2},\quad i = 1, \cdots, N_0,$$

可得

$$\omega/\alpha_i = \mathrm{ctg}(D_i\omega),$$

所以 $D_i\omega \in \left(0, \frac{\pi}{2}\right]$, 这样根据 $|H(\omega)|$ 的表达式, 可得

$$1/|H_i(\omega)| = D_i\omega/\sin(D_i\omega).$$

由于当 $D_i\omega \in \left(0, \frac{\pi}{2}\right]$ 时, 有

$$1 \leq D_i\omega / \sin(D_i\omega) \leq \frac{\pi}{2},$$

根据定理 1 可得, 当 $-\left(D_i \sum_{l \in L} R_{li} K_l \sum_{l \in N} R_{lr}\right) / u_i'' < 1$ 时, 系统在平衡点是局部渐近稳定的 □

推论 3　假设系统的效益函数

$$u_i(x_i) = w_i \log x_i(t),$$

w_i 为正的常数 系统平衡点是 (p_l^*, x_i^*), 系统在平衡点局部渐近稳定的充分条件为

$$\left(D_i \sum_{l \in L} R_{li} K_l \sum_{l \in N} R_{lr} x_r^*\right) < q_i^*, \quad i = 1, \cdots, N_0,$$

这里 $q_i^* = \sum_{l \in L(i)} p_l^*$ 为系统在平衡点对应的连接价格

5　仿真实验

下面通过仿真验证前面得出的系统渐近稳定性结论 假设网络系统中有 2 个连接节点和 5 个源节点, 源节点的窗口大小为: $w_i (i = 1, 2, 3, 4) = 0.002\,5, w_5 = 0.005$. 网络通信时延分别为 $D_1 = 20$ ms, $D_2 = 30$ ms, $d_1 = d_2 = D/2$, 连接节点服务能力分别为 $c_1 = 1$ kb/ms, $c_2 = 0.8$ kb/ms. 源节点 $x_1 \sim x_5$ 共享第 1 个连接节点, 源节点 $x_2 \sim x_5$ 共享第 2 个连接节点, 这样 $R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$. 由式(5)计算得出系统平衡速率分别为 (0.2, 0.16, 0.16, 0.16, 0.32), 平衡拥塞率为 (0.012 5, 0.003 125). 假设连接接点的控制增益分别为 $K_1 = 0.000\,4$, $K_2 = 0.000\,05$, 根据推论 3 可知系统在平衡点渐近稳定

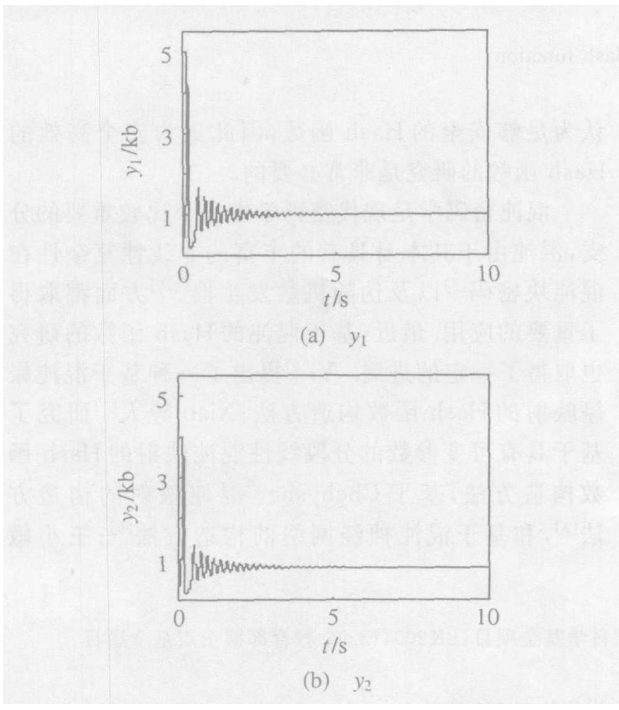

图 2　网络负载时刻图

假设源节点初始速率任意, 计算机仿真得到的网络负载时刻图(图 2) 表明连接节点的传输能力达到最大值, 系统渐近稳定

6　结　　语

本文基于网络优化原理, 建立了一个在网络的源节点和连接节点都是动态变化的 Internet 拥塞控制算法 应用多变量频域控制理论, 分析了动态 Internet 拥塞控制算法在平衡点的渐近稳定性 通过计算机仿真验证了结论的有效性 本文结论为如何构建一个动态 Internet 拥塞控制算法来保证网络的服务质量提供了坚实的理论基础

参考文献(References)

[1] Jacobson V. Congestion Avoidance and Control [A]. *Proc of SIGCOMM'88* [C]. Stanford, 1988: 312-329.

[2] Floyd S, Jacobson V. Random Early Detection Gateways for Congestion Avoidance [J]. *IEEE/ACM Trans on Networking*, 1993, 1(4): 397-413.

[3] Feng W, Kandlur D, Saha D, et al. A Self-configuring RED Gateway [A]. *Proc of the IEEE INFOCOM'99* [C]. New York: IEEE Press, 1999.

[4] Low S H, Paganini F, Doyle J. Internet Congestion Control [J]. *IEEE Control System Magazine*, 2002, 22(1): 28-43.

[5] Floyd S, Gummadi R, Shenker S. *Adaptive RED: An Algorithm for Internet the Robustness of RED's Active Queue Management* [R]. http://www.icir.org/floyd/papers/adaptiveRed.pdf. 2001-01-19.

[6] Kelly F P, Maulloo A, Tan D. Rate Control for Communication Networks: Shadow Prices, Proportional Fairness, and Stability [J]. *J of the Operational Research Society*, 1998, 49(6): 237-252.

[7] Athuraliya S, Low L IV, Yin Q. REM: Active Queue Management [J]. *IEEE Network Magazine*, 2001, 15(3): 48-53.

[8] Kelly F P. Modele for a Self-managed Internet [J]. *Pilosophical Trans of the Royal Society*, 2000, 358(8): 2335-2348.

[9] Fendick F W, Rodrigues M A, Weiss A. Analysis of a Rate-based Feedback Control Strategy for Long Haul Data Transport [J]. *Performance Evaluation*, 1992, 16(1): 67-84.

[10] Johari R, Tan D. End-to-end Congestion Control for the Internet: Delays and Stability [J]. *IEEE/ACM Trans Networking*, 2001, 9(6): 818-832.

[11] Tian Y P, Yang H Y. Stability of the Internet Congestion Control with Diverse Delays [J]. *Automatica*, 2004, 40(9): 1533-1541.

(下转第 1248 页)

图 5(a) 和 5(b) 分别给出了 $d = 8, 16$ 时 SCH 的 $n(k)$ 分布情况. 将同样的实验用于MD5, 图 5(c) 和 5(d) 分别给出了 $d = 8, 16$ 时MD5 的 $k - n(k)$ 分布情况. 从图中可以看出, 在摘要比特 8 和 16 情况下, SCH 的抗碰撞性均好于传统的MD5.

5 结 论

本文提出一种基于时空混沌系统的Hash 函数构造方法. 通过基于分段线性函数的单向时空耦合映像格子和基于迭代Logistic 映射的初始状态, 生成函数来实现明文信息和密钥信息的混淆和扩散, 并基于密码块连接模式实现任意长度明文消息到 128 位摘要之间的单向Hash 函数. 相关实验表明, 该Hash 函数具有很好的明文和密钥敏感性, 以及足够大的密钥空间和较好的抗碰撞性. Hash 函数在安全性能上的这些优点使其适合于数据签名和认证等诸多领域.

参考文献(References)

[1] Vanstone S A, Menezes A J, Oorschot P C. *Handbook of Applied Cryptography* [M]. CRC Press, 1996.

[2] Wang X Y, Yu H B. How to Break MD5 and Other Hash Functions [A]. *Advances in Cryptology - Eurocrypt* [C]. LNCS 3494, 2005: 19-35.

[3] Pareek N K, Patidar V, Sud K K. Discrete Chaotic Cryptography Using External Key [J]. *Physics Letters A*, 2003, 309(1-2): 75-82.

[4] Stojanovski T, Kocarev L. Chaos-based Random Number Generators — Part I: Analysis [J]. *IEEE Trans on Circuits and Systems I — Foundamental Theory and Application*, 2001, 48(3): 281-288.

[5] Stojanovski T, Kocarev L. Chaos-based Random Number Generators— Part II: Practical Realization [J]. *IEEE Trans on Circuits and Systems I — Foundamental Theory and Application*, 2001, 48(3): 382-385.

[6] Yi X. Hash Function Based on Chaotic Tent Maps [J]. *IEEE Trans on Circuits and Systems — II: Express Briefs*, 2005, 52(6): 354-357.

[7] Xiao D, Liao X F, Deng S J. One-way Hash Function Construction Based on the Chaotic Map with Changeable-parameter [J]. *Chaos Solitions and Fractals*, 2005, 24(1): 65-71.

[8] Xiao D, Liao X F, Tang G P, et al. Using Chebyshev Chaotic Map to Construct Infinite Length Hash Chains [A]. *Int Symposium on Circuits and Systems* [C]. Vancouver: IEEE, 2004: 11-12.

[9] Xiao D, Liao X F. A Combined Hash and Encryption Scheme by Chaotic Neural Network [A]. *Int Symposium on Neural Network* [C]. Dalian: Springer, 2004: 633-638.

[10] 王小敏, 张家树, 张文芳. 基于广义混沌映射切换的单向Hash 函数构造[J]. ***物理学报***, 2003, 52(11): 2737-2742.
(Wang X M, Zhang J S, Zhang W F. One Way Hash Function Construction Based on the Extended Chaotic Maps Swith [J]. *Acta Physica Sinica*, 2003, 52(11): 2737-3742.)

[11] 李红达, 冯登国. 复合离散动力系统与Hash 函数[J]. ***计算机学报***, 2003, 26(4): 460-464.
(Li H D, Feng D G. Composite Nonlinear Discrete Chaotic Dynamical Systems and Keyed Hash Functions [J]. *Chinese J of Computers*, 2003, 26(4): 460-464.)

[12] 单梁, 李军, 王执铨. 时空混沌序列在语音保密通信中的应用[J]. ***东南大学学报***, 2004, 34(增): 20-23.
(Shan L, Li J, Wang Z Q. Speech Secure Communications Using Spatiotemporal Chaotic Sequence [J]. *J of Southeast University*, 2004, 34(S): 20-23.)

[13] Wang S H, Kuang J Y, Li J H, et al. Chaos-based Communications in a Large Community [J]. *Physical Review E*, 2002, 66(6): 1-4.

[14] Papadimitriou S, Bountis T, Mavroudi S, et al. Probabilistic Symmetric Encryption Scheme for Very Fast Secure Communication Based on Chaotic Systems of Difference Equations [J]. *Int J on Bifurcation and Chaos*, 2001, 11(12): 3107-3115.

(上接第 1243 页)

[12] Massoulie L. Stability of Distributed Congestion Control with HeteHogeneous Feedback Delays [J]. *IEEE Trans on Automatic Control*, 2002, 47(6): 495-902.

[13] Vinnicombe G. *On the Stability of End-to-end Congestion Control for the Internet* [R]. CUED/F-INFENG/TR. 398. http://www-control.eng.cam.ac.uk/gv/internet, 2001-11-17.