

多 TCP 协议多链路端拥塞控制特性研究

陈晓龙^{1,2} 章 云¹ 刘 治¹

(广东工业大学自动化学院 广州 510090)¹ (茂名学院计算机与电子信息学院 茂名 525000)²

摘 要 当多链路端网络模型中包含有多种 TCP 协议的数据源端时,不同源端根据不同的反馈信号调整发送速率,无法保证网络平衡点的存在性和唯一性及带宽分配的公平性。针对不同源端不同反馈价格机制,引入价格映射函数,建立了具有不同价格映射函数的对偶优化模型。证明了在适当假设下该模型平衡点是存在的。提出并证明了保证网络平衡点唯一性的价格映射函数设计条件。同时在期望带宽分配公平性的平衡点下给出了网络允许的最大往返延迟时间。

关键词 多 TCP 协议,价格映射函数,对偶优化模型,平衡点,公平性

中图法分类号 TCP273 **文献标识码** A

Study of Congestion Control Characteristic on Multi-TCP Protocols and Multi-links

CHEN Xiao-long^{1,2} ZHANG Yun¹ LIU Zhi¹

(School of Automation,Guangdong University of Technology,Guangzhou 510090,China)¹

(School of Computer and Electronics and Information,Maoming College,Maoming 510090,China)²

Abstract When multi-TCP protocol ends react to different pricing signals sharing the multi-links network, the existence and the unique equilibrium and the fairness of the bandwidth allocation may no longer be guaranteed. Because different sources react to different feedback price, a dual optimization model was modeled with price mapping function which describes the relation among different protocol price. The existence of equilibrium in general multiprotocol networks under mild assumptions was proved. The condition of the price mapping function was proposed and proved to ensure the network unique equilibrium. The maximum allowable RTT was obtained by the equilibrium of the expected bandwidth allocation simultaneity.

Keywords Multi-TCP protocols, Price mapping function, Dual optimization model, Equilibrium, Fairness

1 引言

早期的网络拥塞控制模型是将复杂的网络结构简化为一个具有相同 TCP 传输协议的单源单链路端网络拓扑。Misra V, Hollot 等人假设 TCP 主要处于拥塞避免阶段和 TCP 的丢包符合泊松分布,在忽略 TCP 窗口限制等因素的影响下建立了基于流体流模型的源端 TCP 拥塞窗口和网络端队列变化的微分方程^[1,2]:

$$\dot{W}_i(t) = \frac{1}{R_i(t)} - \frac{W_i(t)W_i(t-R(t))p_i(t-R(t))}{2R_i(t-R(t))}$$
$$\frac{dq(t)}{dt} = -C + \sum_{i=1}^N \frac{W_i}{R_i(q)}$$

该模型一定存在平衡点, Hollot 等人在平衡点对其进行了局部线性化。在此线性模型基础上,出现了很多 AQM 控制策略及相关稳定性分析^[3,4]。

针对具有相同 TCP 协议的多链路端的更一般的网络拓扑结构, Kelly, Low^[5,6] 等人引入资源优化方法,将拥塞控制问题视为分布式的资源分配问题。它由用户源端和网络链路这

两个组件构成。用户源端可以用它的效用函数来区分其流量特征。用户期望通过拥塞控制其最大化利益,即效用减去带宽代价。网络链路端则是由一系列具有固定容量的链路组成。这些网络资源由用户共享。因此,网络拥塞控制问题可以归纳为一个带线性限制的非线性规划问题。

$$\max_x U(x) \quad s. t. Ax \leq c, x \geq 0$$

控制目标就是选择源端发送速率(效用函数 $U(x)$),在链路容量限制条件下最大化聚合效用函数。通过这个优化框架,我们可以获得用户发送速率的全局优化集合。由于是凸集上的凹目标最优化问题,由非线性规划的 kuhn-tucker 定理可知,只要在路由矩阵满秩的情况下,系统存在平衡点,并且该平衡点就是用户和整个网络系统的最优解。

基于优化理论的分布式拥塞控制的研究成果极为丰富^[7-9],主要可以分为三类:第一类是基于频域方法考虑传输时延影响的局部平衡稳定性分析控制;第二类是不考虑时延情形下一般网络结构下的非线性全局平衡稳定性分析控制;第三类是同时考虑时延和非线性影响下的平衡稳定性分析控

到稿日期 2008-06-13 本文受国家广东省联合基金(U0735003),国家自然科学基金基金项目(编号:60604006),教育部博士点基金(20070562005)资助。

陈晓龙(1971—),男,副教授,博士生,从事网络拥塞控制、非线性控制的研究,E-mail: xlycxl@126.com;章 云(1963—),男,教授,博士,博士生导师,从事智能控制与信息处理技术、控制网络与集成、机器人技术与自动化装备的研究。

制。

然而,当多链路端网络模型中包含有多种 TCP 协议的数据源端时,上述的丰富的研究成果将不再有效。甚至由于不同协议根据不同的反馈信号调整发送速率,网络平衡点的存在性和唯一性都得不到保证^[10],某些情况下网络可有多个平衡点,甚至是无穷多个平衡点^[12]。这样严重影响了系统的稳定性分析和带宽分配的公平性研究。所以希望找到多协议共享同一网络的平衡点的存在性和唯一性的设计条件。

2 多种 TCP 源多链路端网络模型

2.1 网络模型

假设网络中所有连接的数量、每条连接的持续时间和路由路径都保持大时间尺度上的稳定性。如图 1 所示,假设所研究网络具有 L 个瓶颈链路端和 J 种 TCP 协议数据源端。第 j 种 TCP 数据源具有 N^j 个数据连接。 (j, i) 表示第 j 种 TCP 源的第 i 个数据连接, $j=1, \dots, J, i=1, \dots, N^j$ 。总的连接数为 $N = \sum_{j=1}^J N^j$ 。我们定义一个具有五元素的网络模型 (C, R, m, U, τ) 。

$C = \{c_1, c_2, \dots, c_L\}$ 表示 L 个瓶颈链路容量向量。 $R = [R^1, \dots, R^J]_{L \times N}$ 表示路由矩阵^[7],

其中 $R^j = \{R_{li}^j\}_{L \times N^j}$, $R_{li}^j = \begin{cases} 1 & (j, i) \text{ 通过链路 } l \\ 0 & \text{没有通过} \end{cases}$

$m(p) = (m_l^j(p_l))_{L \times J}$ 表示价格映射矩阵。

其中 p_l 表示第 l 个链路端通用的网络拥塞价格(队列长度), $p = \{p_1, p_2, \dots, p_L\}$ 。 $m_l^j(p_l)$ 表示瓶颈链路 l 的通用价格映射至第 j 种 TCP 协议的价格^[10], 它依赖于链路和协议。由于不同种类的 TCP 端响应不同的链路价格, 如 reno 协议端根据链路端的丢包调整自身的数据发送速度, FAST 协议端根据链路缓冲端的排队延时进行调整^[14]。我们用价格映射关系来描述这种不同响应机制。将瓶颈链路中通用的网络拥塞价格 p_l (队列长度) 映射成不同种类协议认可的价格(丢包概率、对列延时等)。 $U = \{U_i^j(x_i^j)\}$ 表示效用函数。 τ 表示传播延时矩阵。

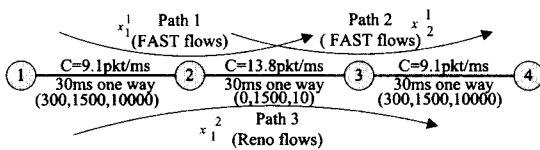


图 1 具有二协议三瓶颈链路

网络拥塞控制的分布式运算可以描述如下^[6]:

假设所有种类的 TCP 流为持续流(Long-lived flow)。对于任给的源端 (j, i) , 在分布式网络环境下能够获得以下数据: 源端发送速率 $x_i^j \geq 0$; 严格凸增效用函数 $U_i^j(x_i^j)$; 往返延时 $\tau_i^j, \tau_i^j = \tau_{if}^j + \tau_{bf}^j$; τ_{if}^j, τ_{bf}^j 分别表示源端前向和后向传播延时。源端累积价格:

$$q_i^j = \sum_{l=1}^L R_{li}^j m_l^j(p_l(t - \tau_{bf}^j)) \quad (1)$$

源端根据以上数据静态调整源端速率公式:

$$x_i^j(t) = U_i^j{}^{-1}(q_i^j(t)) \quad (2)$$

对于任给的链路 $l \in L$, 能够获得以下数据:

链路 l 的带宽容量为 $c_l > 0$, j 种 TCP 类到达速率

$$y_l^j = \sum_{i=1}^{N^j} R_{li}^j x_i^j(t - \tau_{bf}^j) \quad (3)$$

$y = \{y_l^j\}_{L \times J}$, $\dot{p}_l(t) = g_l(y(t), p_l(t))$ 由式(3)和 c_l 可动态算出通用的网络拥塞价格 p_l (队列长度)。根据价格映射函数计算出各种 TCP 协议的价格 $m_l^j(p_l)$ 。

例 1: 如图 1 所示, 当同一网络具有 TCP fast 和 TCP reno 协议和 3 个瓶颈链路时, 假设 TCP reno 流链路端的 AQM 策略为 RED 算法:

$$p(b) = \begin{cases} 0 & b \leq \underline{b} \\ (b - \underline{b}) / (K(\bar{b} - \underline{b})) & \underline{b} \leq b \leq \bar{b} \\ 1/K & b \geq \bar{b} \end{cases}$$

$(\underline{b}, \bar{b}, K)$ 分别表示最小, 最大缓冲队列长度和比例系数。3 个链路端参数 $(\underline{b}, \bar{b}, K)$ 分别是: $(300, 1500, 10000)$, $(0, 1500, 10)$, $(300, 1500, 10000)$ 。假设链路容量 $c_1 = c_3 \leq c_2 \leq 2c_1$, 那么当 FAST 流先走时, 链路 2 先饱和, 当 RENO 流加入时, 由于链路 2 的比例因子较大, 因此链路 2 会产生较多丢包, RENO 流受到挤压, 带宽分配较小。当 RENO 流先走时, 链路 1, 3 先饱和, 由于其比例因子小, 因此丢包概率小, 缓冲队列长度大, 当 FAST 流加入时, 链路 1, 3 会产生较大排队延迟, FAST 流受到挤压, FAST 流分配带宽小。可见由于网络中存在不同的协议会存在不同的平衡点, 从而造成带宽分配的严重不公平性和系统的不稳定性。

2.2 最优化模型及网络平衡点

2.2.1 最优化模型

网络系统采取控制策略也具有两个目标: 一方面, 网络系统希望所有用户获得的满意程度尽可能大, 即所有用户的效用函数之和最大; 另一方面, 网络系统希望拥塞反馈信号占用的网络资源尽可能小, 即所有链路在单位时间内产生的拥塞反馈信号总和最小。因此, 对于网络系统而言, 最优化问题可以描述为^[6]:

$$\max \{ \sum_{j,n} (U_i^j(x_i^j) - x_i^j q_i^j) \} \quad (4)$$

其中 $y \leq C$

由于约束条件是凸集及相应的凹目标函数, 由非线性规划的 kuhn-tucker^[6]定理可知平衡点存在的充分必要条件是:

$$\begin{aligned} U_i^j(x_i^j) &= q_i^j \quad P(y(p) - c) = 0 \\ y(p) &\leq C, p \geq 0 \end{aligned} \quad (5)$$

其中: $P = \text{diag}(p_l)$ 是一个对角矩阵。

当系统处于平衡点时, 发送速率和累积价格保持大时间尺度上的稳定, 所以满足:

$$x_i^j = (U_i^j)^{-1}(q_i^j) \quad (6)$$

2.2.2 网络平衡点定义及存在性

定义 1 满足式(1)、(6)、(5)的价格 p 为网络的平衡点, 其平衡点集合为:

$$E = \{p \in R_+^L \mid P(y(p) - c) = 0, y(p) \leq c\} \quad (7)$$

由式(5)可知, 当 $y_l(p) = c_l$ 时, 有 $p_l > 0$ (8)

定义满足式(8)的所有链路 l 的主动约束集合:

$\hat{L} = \hat{L}(p^*) \subset L$, 在这个简约的集合里定义其平衡点雅可比矩阵:

$$\hat{J}(\hat{p}) = \frac{\partial y(\hat{p})}{\partial \hat{p}} = \sum_j \hat{R}^j \frac{\partial x_i^j}{\partial q_i^j}(\hat{p}) (\hat{R}^j)^T \frac{\partial m_l^j}{\partial p}(\hat{p}) \quad (9)$$

$$\frac{\partial x_i^j}{\partial q_i^j} = \text{diag}((\partial^2 U_i^j / \partial (x_i^j)^2)^{-1}), \frac{\partial m_l^j}{\partial p} = \text{diag}(\partial m_l^j / \partial p_l)$$

作适当的假设:

假设 A1: 效用函数是严格凸增函数和二次连续可导, 价格映射函数连续可导和严格增函数。有 $m_l^i(0)=0$ 。

假设 A2: 对 $\forall \epsilon > 0$, 存在一个 $p_{\max} > 0$, 对所有 (i, j) , 当 $R_{li}^j = 1$ 和 $p_l > p_{\max} > 0$, 有 $x_l^i(p) < \epsilon$ 。

假设 A3: 每个链路 l 拥有一个单链路流 (i, j) , 且 $(U_l^i)'(c_l) > 0$ 。该假设表明当链路 l 的价格足够小时, 通过其链路的速率将超过其容量, 这个假设确保主动约束集合包含了所有链路。

定理 1 假设 A1, A2 成立, 对给定任意网络 (C, R, m, U, τ) , 一定存在一个平衡点。

证明: 由假设 A2 可知, 网络平衡点 $\bar{p}_l \leq p_{\max}$, 否则可令 $\epsilon = \min_i c_l / N$, 当 $\bar{p}_l > p_{\max} > 0$, 有 $y(p) < c$ 与式(5)矛盾。定义 $p_{-l} = (p_1, \dots, p_{l-1}, p_{l+1}, \dots, p_L)$, $F(p) = Rx(p) - c$

$F(p)$ 写为 $F(p_l, p_{-l})$, 定义 $h_l(p_l, p_{-l}) = -F^2(p_l, p_{-l})$, 对固定 p_{-l} , $h_l(p_l, p_{-l})$ 是自变量 p_l 的拟凹连续函数, p_l 所属的 $[0, p_{\max}]$ 集合是紧且凸的, 由 Nash 平衡点^[15]存在定理知一定存在一个 Nash 平衡点使得 $\bar{p}_l = \max_{p_l \in [0, p_{\max}]}$ $h_l(p_l, p_{-l})$ 。

2.3 网络平衡点唯一性存在条件

定义 2 网络模型 (C, R, m, U, τ) 在平衡点雅可比矩阵式(9)非奇异, 则该平衡点为局部唯一, 如果该雅可比矩阵所有的特征值为负, 该平衡点是局部稳定的。如果所有平衡点都局部唯一, 该网络为正则网络^[10]。

定义 3 对所有平衡点 $p \in E$ 定义索引^[11]:

$$I(p) = \begin{cases} 1 & \det(J(p)) > 0 \\ -1 & \det(J(p)) < 0 \end{cases}$$

定义 4^[9] 定义 $f(p) = Rx(p(t))$ 是关于 p 的连续递减函数, 定义对偶优化模型的梯度搜索算法:

$$\dot{p}(t) = k[f(p(t - \tau_m)) - c] \quad (10)$$

定义递增函数: $F(u) = f(\bar{p} - u) - c$, 由平衡点定义知 $F(0) = 0$ 。

引理 1 (Poincare-Hopf index 定理^[16]) 设 D 是 R 上的开子集, $v: D^L \rightarrow R^L$ 上的光滑向量场, $\frac{\partial v}{\partial p}$ 是平衡点上的非奇异雅可比矩阵, 如果存在 $G \subseteq D^L$, 使得轨迹向一到 G 的边界后就会反向向内部靠拢, 则 $\sum_{p \in G} I(p) = (-1)^L$ 。

定理 2 假设 A1, A2, A3 成立, 任何正则网络, 当 $\tau_m \leq \left[\frac{p_{\min} - \bar{p}}{F(\bar{p} - p_{\max})}, \frac{p_{\max} - \bar{p}}{F(\bar{p} - p_{\min})} \right]$ 有 $\sum_{p \in E} I(p) = (-1)^L$ 。 $\bar{p}$ 为期望的平衡点。

证明: 由 A3 知存在 $p_{\min}$, 使得对任意 $p_l < p_{\min}$ 有 $y(p) > c$ 。令 $G = [p_{\min}, p_{\max}]$, 显然平衡点 $\bar{p} \in G$ 。令 $\tau_m = \max(\tau_l^i)$, 当处于平衡点时 $f(\bar{p}) = c$ 。 $\delta p = \bar{p} - p_{\min}$, 则对任意 $t > 0$, 有 $\dot{p}(t) \leq F(\delta p)$ 。定义 $\Delta p = \tau_m F(\delta p)$ 。若网络不存在延时, 由式(10)知应满足 $(p - \bar{p})\dot{p} < 0$ 。因为延时的影响, 若当 $t > \tau_m$ 时有 $p(t) > \bar{p} + \Delta p$ 。那么对任意的对 $\sigma \in [0, \tau_m]$, 有 $p(t - \sigma) > \bar{p}$, 由式(10)知 $\dot{p}(t) < 0$ 。所以要求 $\tau_m \leq \frac{p_{\max} - \bar{p}}{F(\bar{p} - p_{\min})}$ 。同理可得 $\tau_m \leq \frac{p_{\min} - \bar{p}}{F(\bar{p} - p_{\max})}$ 。由引理 1, 定理 2 结论成立。

推论 3 假设 A1, A2, A3 成立, 则一个正则网络的平衡点是全局唯一的当且仅当 E 中的每个平衡点有索引 $(-1)^L$ 。尤其若所有平衡点是局部稳定的, 则平衡点个数唯一。

证明: 如果 E 中的每个平衡点有索引 $(-1)^L$, 由定理 2 可

知其个数只能唯一。同理, 由定义 2 知局部稳定意味其雅可比值为负, 因此只有其个数唯一时, 定理 2 结论成立。

定义 5 向量 $\sigma = \{\sigma_1, \sigma_2, \dots, \sigma_L\}$ 是一个置换, 指所有向量元素 σ_l 取值于 $\{1, 2, \dots, L\}$ 且互不相同。 σ^{-1} 是其唯一的逆置换。 $l = \{1, 2, \dots, L\}$ 为单位置换^[10]。定义 $\dot{m}_l^i = dm_l^i / dp^l$ 。

定理 4 假设 A1, A2, A3 成立, 正则网络的平衡点是全局唯一, 当对任意的 $j \in \{1, \dots, J\}$ 和任意在 $\{1, \dots, L\}$ 置换 σ, k, n , 有:

$$\prod_{l=1}^L \dot{m}_l^{[\sigma(j)]} + \prod_{l=1}^L \dot{m}_l^{[\sigma(j)]} \geq \prod_{l=1}^L \dot{m}_l^{[\sigma(j)]} \quad (11)$$

证明: 由定理 3 可知只要证明对任何每个平衡点有索引 $I(p) = (-1)^L$, 由于 $\det(J(p)) = (-1)^L \det(-J(p))$, 所以只需证明 $\det(-J(p)) > 0$ 。因为: $(-J(p)) = -\sum_j R^j D^j$

$(R^j)^T \frac{\partial m^j}{\partial p}(p) = \sum_j B^j M^j$, 其中: $M^j = M^j(p) = \frac{\partial m^j}{\partial p}(p)$, 是 $L \times L$ 方阵, $B^j = B^j(p)$ 其元素 $B_{kl}^j = \sum_i R_{li} R_{li} (-\partial^2 U_l^i / \partial (x_l^i)^2)^{-1}$ 表明同时通过链路 k, l 端的 j 种类型的 TCP 源端 i 的项进行求和。

$$\det(-J(p)) = \det(\sum_j B^j M^j) = \sum_k \text{sgn}(k) \prod_{l=1}^L \sum_{i=1}^L (B^j M^j)_{k_l l} \quad (12)$$

$k = \{k_1, k_2, \dots, k_L\} \in \{1, 2, \dots, L\}$ 表示共有 $L!$ 种置换。

定义 5 π 表示路径, 是一个二进制序列, 如果经过链路 l , 则有 $\pi_l = 1$ 。 $\Pi(k, l) = \{\pi_k = \pi_l = 1\}$, 表示同时经过链路 k, l 的路径的集合。 $I_\pi^j = \{i | R_{li} = 1, \pi_l = 1\}$ 表示类型 j 经过路径 π 的源端 i 的集合。 $r_\pi^j = r_\pi^j(p) = \sum_{i \in I_\pi^j} (-\partial^2 U_l^i / \partial (x_l^i)^2)^{-1}$, 表示经过路径 π 的所有源端的 i 项的和。所有 $B_{kl}^j = \sum_{\pi \in \Pi(k, l)} r_\pi^j$ 表示所有经过链路 k, l 的路径的源端 i 的项和。由定义 5, 式(12)可改为:

$$\det(-J(p)) = \det(\sum_j B^j M^j) = \sum_k \text{sgn}(k) \prod_{l=1}^L \sum_{i=1}^L \left(\dot{m}_l^j \sum_{\pi \in \Pi(k_l, l)} r_\pi^j \right) \quad (13)$$

考虑到序列 $a_{ij}, j \in J_i, i = 1, 2, \dots, I$, 其中 J_i 是一个依赖于 i 有限个数的下标, 有 $\prod_{i=1}^I \sum_{j \in J_i} a_{ij} = \sum_j \prod_{i=1}^I a_{ij}$, 其中 $\bar{j} = (j_1, \dots, j_I)$, 右边项表示对笛卡尔集合 $(J_1 \times \dots \times J_I)$ 的所有可能组合求和。交换连乘和连加符号, 式(13)可写为:

$$\det(-J(p)) = \sum_k \text{sgn}(k) \sum_j \prod_{l=1}^L \left(\dot{m}_l^{j_l} \sum_{\pi \in \Pi(k_l, l)} r_\pi^{j_l} \right) \quad (14)$$

其中 $j = \{j_1, \dots, j_L\}$ 表示所有可能的排列。进一步交换连乘和连加符号得:

$$\det(-J(p)) = \sum_k \text{sgn}(k) \sum_j \mu(j) \sum_{\pi \in \Pi(k, l)} \rho(j, \pi) \quad (15)$$

其中: $\mu(j) = \prod_{l=1}^L \dot{m}_l^{j_l} \rho(j, \pi) = \prod_{l=1}^L r_{\pi_l}^{j_l} \pi = (\pi^1, \dots, \pi^L)$

$$\pi \in \Pi(k, l) \text{ 表示 } \pi^l \in \Pi(k_l, l), l = 1, 2, \dots, L \quad (16)$$

表示经过链路 k_l, l 的 L 条路径的所有组合。所以有

$$\det(-J(p)) = \sum_j \sum_{\pi} C(j, \pi) \rho(j, \pi) \quad (17)$$

其中 $C(j, \pi) = \sum_k 1(\pi \in \Pi(k, l)) \text{sgn}(k) \mu(j)$, 由式(17)可知 $\det(-J(p))$ 的值是基于下标 (j, π) 系数为 $C(j, \pi)$, 项为 $\rho(j, \pi) > 0$ 的值的和。 $1(a)$ 表示 a 为真时值为 1, 否则 0。

引理 2 如果式(17)中项 $\rho(j, \pi)$ 存在整数: $a, b \in \{1, \dots, L\}$, 且有 $j_a = j_b$ 和 $\pi^a = \pi^b$ 时, 那么 $C(j, \pi) = 0$ 。

0	0	0	1	0	0
0	-1	0	-1	0	0

表1说明了当 j, π, σ 确定时,根据 k 的6种不同排列生成第2列不同的路径组合,根据 $1(\sigma(\pi) \in \Pi(k, l))$ 计算第3列得到能够产生3个不为零的项。其中两个为正项且只有当 $k=3, 2, 1$ 时,会产生一个系数为负的项。由于具有相同的 $\mu(\sigma(j))$,因此总可由其中的一个正系数项抵消。由于当 σ 发生变化时表1的第1, 2, 4列并不会改变,表2是根据 σ 的6种不同组合对表1第3列进一步计算得到的相应的36种结果。从表2中可看到第4列和第5列都只产生一个负数项,可由其具有相同项得正系数项抵消。只有当 $\sigma=(1, 3, 2)$ 时有两个系数为负的项,其 $k=(2, 1, 3)$ 和 $n=(3, 2, 1)$ 。说明此时有 $\sigma(\pi) \in \Pi(k, l)$ 和 $\sigma(\pi) \in \Pi(n, l)$,由式(16)可得到 $\sigma(\pi) \in \Pi(l, l)$, $\sigma(\pi) \in \Pi(k, n)$ 和 $\sigma(\pi) \in \Pi(n, k)$ 。由 $\sigma(\pi) \in \Pi(l, l)$ 正好是表2的第2列第1行为正项,且有相同的 $\mu(\sigma(j))$ 可与其第3列第3行负项抵消。由于 $\sigma(\pi) = \{111, 110, 101\}$, $\Pi(k, n) = \{\Pi(2, 3), \Pi(1, 2), \Pi(3, 1)\}$,将 $\Pi(k, n)$ 按第二项顺序排: $\Pi(k', l) = \{\Pi(3, 1), \Pi(1, 2), \Pi(2, 3)\}$, $\sigma'(\pi) = \{101, 110, 111\}$,得到其 $k' = \{3, 1, 2\}$ $\sigma' = \{2, 3, 1\}$,查表2知由 (σ', k') 所决定的项为 $\mu(\sigma'(j))$ 系数为正。同理将 $\sigma(\pi) \in \Pi(n, k)$ 重排可得到 $k'' = \{2, 3, 1\}$ $\sigma'' = \{3, 1, 2\}$ 查表2知 (σ'', k'') 所决定的项为 $\mu(\sigma''(j))$ 系数为正。所以要想式(18)的系数为正必须要求 $\mu(\sigma'(j)) + \mu(\sigma''(j)) > \mu(\sigma(j))$ 成立。代入得:

$$\mu(2, 2, 1) + \mu(2, 1, 2) > \mu(1, 2, 2), \text{将式(15)代入得:} \\ m_1^2 m_2^2 m_3^1 + m_1^1 m_2^1 m_3^2 > m_1^1 m_2^2 m_3^2 \quad (22)$$

该例子说明了为了保证 $\det(-J(p)) > 0$,要求其按行列式展开每一项系数都大于必须满足的条件。显然若在设计价格映射函数时能满足定理4的条件,即不同链路上所有价格映射函数导数组合乘积满足式(11),显然满足式(22)。

3 不同 TCP 价格映射函数设计

定理4的应用价值在于在已知网络链路容量 c ,具有多种TCP协议的路由矩阵 R 和源端效用函数 U 的情况下,为了保证网络平衡点的唯一性可在该定理指导下设计各种TCP协议源端的在各链路瓶颈端的价格响应函数。设计时对任意 $l=1, 2, \dots, L, j=1, 2, \dots, J$,当取的一个 a_l 要求所设计的价格映射函数满足 $\dot{m}_l^j \in [a_l, 2^{1/L}]$,这样设计价格函数就可以一定满足式(11),从而保证了网络平衡点的唯一性。但由于式(11)要求所有不同两个链路端价格函数导数的不同组合乘积必须大于其它组合的乘积,这样的要求过于保守。其实在定理4的证明过程中我们发现,为了保证行列式的系数为正,只是要求相关链路的价格函数组合满足式(21)即可保证平衡点的全局唯一性。所以在已知路由矩阵的情况下可大大简化定理4。例如图1所示的网络拓扑中,只有 $\rho(j, \pi) = r_{110}^1 r_{011}^1 r_{111}^2$ 这样一组组合,其他路径组合情况都不存在。根据表1、表2的运算方法可以得到只要满足下式即可。

$$\mu(2, 1, 1) + \mu(1, 1, 2) > \mu(1, 2, 1) \quad (23)$$

而不要求满足式(11)所有可能组合的情况。相对式(11)减少了两个不等式,降低了定理的保守性。具体说明如下:

设置FAST流的价格映射函数: $m_l^i(p_l) = p_l = b_l/c_l$

(下转第103页)

证明:当 j, π 确定时,不失一般性可假设 $j_1 = j_2, \pi^1 = \pi^2$,由式(16)知: $\pi^1 \in \Pi(k_1, 1), \pi^2 \in \Pi(k_2, 2)$,所以路径 π^1, π^2 经过链路 $1, 2, k_1, k_2$ 。所以由 $\pi^1 \in \Pi(k_2, 1), \pi^2 \in \Pi(k_1, 2)$,因而一定存在另一个置换 $\hat{k}$,有 $\hat{k}_1 = k_2, \hat{k}_2 = k_1, \hat{k}_l = k_l (l \geq 3)$,使得 $\text{sgn}(k) = -\text{sgn}(\hat{k})$,所以使得 $C(j, \pi) = 0$ 证毕。所以只有 $\rho(j, \pi)$ 中所含的乘积项 $r_{\pi_l}^{j_l}$ 都不相同时,其系数才不为0。

定义6 定义 Θ 为 $\rho(j, \pi)$ 中所含的乘积项 $r_{\pi_l}^{j_l}$ 都不相同的 (j, π) 的组合集合。定义置换 $\sigma(j, \pi) = (\sigma(j), \sigma(\pi))$ 。

定义 Θ_0 为 Θ 置换后最大的不同元素的集合。

由定义6可知式(17)可写为:

$$\det(-J(p)) = \sum_{(j, \pi) \in \Theta_0} D(j, \pi) \rho(j, \pi) \quad (18)$$

其中: $D(j, \pi) = \sum_{\sigma} \sum_k 1(\sigma(\pi) \in \Pi(k, l)) \text{sgn}(k) \mu(\sigma(j))$,由置换定义

$$D(j, \pi) = \sum_{\sigma} \sum_k 1(\pi \in \Pi(k, \sigma^{-1})) \text{sgn}(k\sigma) \mu(\sigma(j)) \quad (19)$$

当 (j, π) 确定时,任取一个 σ ,假设存在一个置换 k 使得 $1(\pi \in \Pi(k, \sigma^{-1})) \text{sgn}(k\sigma) = -1$,则一定可取另一个置换 $\hat{k} = \sigma^{-1}$,使得 $1(\pi \in \Pi(\hat{k}, \sigma^{-1})) \text{sgn}(\hat{k}\sigma) = 1$ 从而与该负项抵消。任取一个 σ ,假设存在两个置换 k, n ,当 $\pi \in \Pi(k, \sigma^{-1}), \pi \in \Pi(n, \sigma^{-1})$ 时,有 $\text{sgn}(k\sigma) = \text{sgn}(n\sigma) = -1$,这样在式(19) $\mu(\sigma(j))$ 中产生两个负项。由式(16)知对 $l=1, 2, \dots, L, \pi^l$ 通过路径 k_l, n_l, σ_l^{-1} ,有: $\pi \in \Pi(\sigma^{-1}, \sigma^{-1})$,因此有 $\text{sgn}(\sigma^{-1}\sigma) = 1$,可抵消其中一个负项。还有:

$$\pi \in \Pi(k, n), \pi \in \Pi(n, k) \quad (20)$$

式(20)意味式(19)有两个非零的系数分别是:

$$1(\pi \in \Pi(k, n)) \text{sgn}(kn^{-1}) \mu(n^{-1}(j)), 1(\pi \in \Pi(n, k)) \text{sgn}(nk^{-1}) \mu(k^{-1}(j))$$

因为 $\text{sgn}(kn^{-1}) = \text{sgn}(k\sigma(n\sigma)^{-1}) = \text{sgn}(k\sigma) \text{sgn}(n\sigma)^{-1} = 1$,同理得 $\text{sgn}(nk^{-1}) = 1$,所以要使式(19)为正必须要求:

$$\mu(n^{-1}(j)) + \mu(k^{-1}(j)) > \mu(\sigma(j)) \quad (21)$$

当式(11)成立时,由式(15)知式(21)一定成立,所以式(18)的系数一定为正。所以 $\det(-J(p)) > 0$ 。定理4证毕。

2.4 定理举例说明

现假设 $L=3, J=2$,当式(18)中的 $\rho(j, \pi) = r_{111}^1 r_{101}^2 r_{110}^2$ 时,即固定 $j=(1, 2, 2); \pi=(111, 101, 110)$ 时,如何计算系数 $D(j, \pi)$,由式(18)知 σ, k 分别有6种不同的组合,现假定 $\sigma=(2, 3, 1)$,有 $\sigma(\pi)=(101, 110, 111)$,见表1。

表1 j, π, σ 确定时系数

	$\Pi(k, l)$	$1(\sigma(\pi) \in \Pi(k, l))$	$\text{sgn}(k)$
$k=1, 2, 3$	$(1, 1)(2, 2), (3, 3)$	1	1
$k=1, 3, 2$	$(1, 1)(3, 2), (2, 3)$	0	-1
$k=2, 1, 3$	$(2, 1)(1, 2), (3, 3)$	0	-1
$k=2, 3, 1$	$(2, 1)(3, 2), (1, 3)$	0	1
$k=3, 1, 2$	$(3, 1)(1, 2), (2, 3)$	1	1
$k=3, 2, 1$	$(3, 1)(2, 2), (1, 3)$	1	-1

同理可计算出表2所列的 j, π 确定时系数。

表2 j, π 确定时系数

$(1, 2, 3)$	$(1, 3, 2)$	$(2, 1, 3)$	$(2, 3, 1)$	$(3, 1, 2)$	$(3, 2, 1)$
0	1	0	1	1	0
0	0	0	0	0	0
0	-1	0	0	-1	0
0	0	0	0	1	0

本文方案的秘密分发简单,参与者需要保存的伪影子仅是一个 $(0, p)$ 上的数而非一个多维空间点,该伪影子秘密可以长期使用,参与者利用其伪影子与公共参数 r 计算其影子;当秘密分发者想更改参与者的影子时,只需更新公告牌上的公开信息即可,可见其秘密分发效率高。

本文方案还具有如下特点:1)它是一个动态的方案,可动态实现参与者的加入与退出,步骤简单,还可以动态改变门限值 t ;2)运算高效,在 $|p|=1024\text{bit}$ 、实现 $(3, 5)$ 门限共享时,Shamir方案的时间消耗约是本文方案的28倍;3)在系统参数变化时,例如参与者的加入/退出、 t 的改变、甚至是共享秘密的修改等,用户所持有的伪影子一直保持不变;4)在同一个参与者集合中,参与者可以使用同一个伪影子多次共享秘密;5)方案是一个安全的 (t, n) 门限秘密共享方案;6)方案动态变化时,秘密分发者与参与者之间无通信量的需求。

参考文献

- [1] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22 (11): 612-613
- [2] Blakley G R. Safeguarding cryptographic keys [C]//Proceedings of National Computer Conference. Montvale, NJ: AFIPS Press, 1979, 48: 313-317
- [3] Stadler M. Publicly verifiable secret sharing [C]//Proc. of Advances in Cryptology — Eurocrypt '96. Berlin: Springer-Verlag,

- 1996, 190-199
- [4] Asmuth C, Bloom J. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory, 1983, 29 (2): 208-210
- [5] Chang T Y, Hwang M S, et al. An improvement on the Lin-Wu (t, n) threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2005, 163(1): 169-178
- [6] Chien H Y, Jan J K, Tseng Y M. A practical (t, n) multi-secret sharing scheme [J]. IEICE Transactions on Fundamentals, 2000, E83-A (12): 2762-2765
- [7] Yang C C, Chang T Y, Hwang M S. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2): 483-490
- [8] Chien H Y, Jan J K, Tseng Y M. A practical (t, n) multi-secret sharing scheme [J]. IEICE Trans on Fundamentals, 2000, E83-A (12): 2762-2765
- [9] Wu T C, He W H. A geometric approach for sharing secrets [J]. Computer & Security, 1995, 14(2): 135-145
- [10] Chor L P, Jing H W, Chong T P. A geometric approach for shared secrets, a refinement [J]. Computers & Security, 1998, 17 (10): 725-732
- [11] 庞辽军, 王育民. 一个基于几何性质的 (t, n) 多重秘密共享方案 [J]. 西安交通大学学报, 2005, 39(4): 425-428
- [12] 庞辽军, 李慧贤, 王育民. 基于几何性质一般访问结构上的多重秘密共享方案 [J]. 计算机科学, 2006, 33(10): 90-93

(上接第91页)

RENO流的价格映射函数: $m_i^p(p_i) = (p_i c_i - b_i) / (K_i (\bar{b}_i - b_i))$

所以价格映射函数矩阵 $\bar{m}^1$ 为单位阵, $\bar{m}_i^2 = c_i / (K_i (\bar{b}_i - b_i))$ 。

由式(15)和式(23)知: 要保证图1网络平衡点唯一性, 价格映射函数(RED参数设置)应满足:

$\bar{m}_1^2 \bar{m}_2^2 \bar{m}_3^2 + \bar{m}_1^1 \bar{m}_2^2 \bar{m}_3^2 > \bar{m}_1^2 \bar{m}_2^2 \bar{m}_3^2$, 将上式代入得:

$$\frac{c_1}{k_1(\bar{b}_1 - b_1)} + \frac{c_3}{k_3(\bar{b}_3 - b_3)} > \frac{c_2}{k_2(\bar{b}_2 - b_2)} \quad (24)$$

结束语 虽然标准的效用函数最大化方法已无法解决具有多协议多瓶颈链路的网络拥塞控制问题。但在引入价格映射函数及满足适当设计条件后重新找到解决网络平衡点存在性、延迟相关和全局唯一性的问题的方法。在得到网络全局唯一平衡点后进一步研究工作应该包括两个方面:(1)多协议多瓶颈链路的网络拥塞控制在平衡点附近的全局稳定性问题。(2)平衡点唯一性表示多协议数据流带宽分配的唯一性, 所以瓶颈链路带宽的公平性分配问题也值得研究。

参考文献

- [1] Misra V, Gong W B, Towsley D. Fluid-based Analysis of a Network of AQM Routers Supporting TCP Flows with an Application to RED [C]//Proceedings of ACM/SIGCOMM, 2000: 151-160
- [2] Holot C V, Misra V, Towsley D, et al. A control theoretic analysis of RED [C]//Proceedings of IEEE INFOCOM, 2003, 5: 1510-1519
- [3] Kim K B. Design of Feedback Control Supporting TCP Based on the State-Space Approach [J]. IEEE TRANS on Automatic Control, 2006, 51(7): 1086-1098
- [4] Tan Liansheng, Zhang Wei, Peng Gang, et al. Stability of TCP/RED systems in AQM Routers [J]. IEEE TRANS Automatic Control, 2006, 51(8): 814-871

- [5] Kelly F, Maoullou A, Tan D. Rate control for communication networks: shadow prices, proportional fairness and stability [J]. Oper. Res. Soc., 1998, 49: 237-252
- [6] Low S H. A duality model of TCP and queue management algorithms [J]. IEEE/ACM Trans. Networking, 2003, 11(4): 525-536
- [7] Lei Ying, Dullerud G E, Srikant R. Global stability of internet congestion controllers with heterogeneous delays [J]. IEEE/ACM Trans. Networking, 2006, 14(3): 579-592
- [8] Zhang Yueping, Kang S-R, Loguinov D. Delay-Independent Stability and Performance of Distributed Congestion Control [J]. IEEE/ACM Trans. Networking, 2007, 15(5): 838-852
- [9] Wang Zhikui, Paganini F. Boundedness and Global Stability of a Nonlinear Congestion Control With Delays [J]. IEEE Automatic Control, 2006, 51(9): 1514-1517
- [10] Tang A, Wang J, Low S H, et al. Network equilibrium of heterogeneous congestion control protocols [C]//Proc. IEEE INFOCOM, 2005: 1338-1349
- [11] Tang A, Wang J, Low S H, et al. Equilibrium of heterogeneous congestion control protocols. Dept. Comput. Sci., California Inst. Technol., Pasadena, CSTR, 2005, 005, 2005
- [12] Tang A, Wang J, Hedge S, et al. Equilibrium and fairness of networks shared by TCP Reno and Vegas/FAST [J]. Telecomm. Syst., 2005, 30(4): 417-439
- [13] Tang A, Wei D, Low S H, et al. Heterogeneous congestion control: Efficiency, fairness and design [C]//Proc. IEEE ICNP, 2006: 127-136
- [14] Wei D, Jin C, Low S H, et al. FAST TCP: Motivation, architecture, algorithms, performance [J]. IEEE/ACM Trans. Netw., 2007, 15(6): 1246-1259
- [15] Dutta D, goel A. Oblivious AQM and Nash Equilibria [J]. IEEE INFOCOM, 2003, 3: 1311-1318
- [16] Aranson S, Belisky G. Introduction to the Qualitative Theory of Dynamical System on Surfaces [J]. Translation of Mathematical Monographs, 1996, 153(6): 123-128