一种基于 Hénon 映射和 Feistel 结构的分组密码算法研究

张 伟[1,2] 韦鹏程[1] 杨华千[1,2]

(重庆教育学院计算机与现代教育技术系 重庆400067)[1]

(重庆大学计算机科学与工程学院 重庆400044)[2]

摘 要 混沌序列具有对初值和系统参数敏感等特点,因此非常适合应用于信息加密。本文在详细分析 Hénon 映射的混沌和密码学特性的基础上,提出一种基于 Feistel 结构和 Hénon 映射混沌分组密码算法,该算法最大的优点加密的轮次和子密钥的构造是基于混沌系统动态更新的,通过子密钥的动态生成,密码系统的随机性、复杂性得到了极大的提高。同时理论和实验表明,该算法具有较高的安全性,能够抵抗差分和线性密码分析。

关键词 混沌加密,分组密码,Feistel 结构,Hénon 映射

A Bock Cryptographic Algorithm Based on Hénon Map and Feistel

ZHANG Wei[1,2] WEI Peng-Cheng[1] YANG Hua-Qian[1,2]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[1]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[2]

Abstract As we all know, chaotic system is sensitive to initial values and system parameters, so it is suitable for information encryption. In this paper, the chaotic and cryptographic properties of the 2-D Hénon map is analyzed and a novel block chaotic cryptographic algorithm based on Feistel and Hénon map is presented. The difference between the presented algorithm and traditional block algorithm is: the number of rounds is dynamically determined by the former ciphertext block, and the subkey also is dynamically generated. The randomicity, complexity and robustness of cryptosystem can be greatly improved by employing a chaotic system within the process of generating the subkeys. At the same time, The results of the security analyses indicate that the algorithm can against the differential and linear attacks and with high security.

Keywords Chaotic encryption, Block cipher, Feistel structure, Hénon map

1 引言

基于混沌理论的数据加密算法是近十年来密码学研究的热点,吸引了不少国内外研究者的注意力,提出了不少的算法,取得了大量的研究成果[1~5]。纵观这些研究成果,混沌的应用主要有四个方面:一是运用混沌同步进行混沌保密通信;二是运用一维或高维混沌所产生的伪随机序列与待加密的明文进行异或运算以产生密文,这是混沌应用于序列密码算法的典型方法;三是将混沌映射作为加密变换的轮函数,将混沌迭代与明文信息相结合以产生密文,这方面的研究因所运用的混沌映射和所采用的结合方法不同而使算法精彩纷呈。四是混沌映射与分组密码中非常经典的 Feistel 结构相结合,以获得具有非常好的扩散和混乱效果。这种应用方法不多见,只在文[6,7]中略有体现,但其应用只是将所选择的混沌映射用于采用 Feistel 结构的分组密码中,而没有将 Feistel 结构与混沌映射有机地结合,也就是说没有充分运用混沌映射的混沌与密码学特性。

本文在详细分析混沌系统 Hénon 映射的基础上,提出一种新颖的基于 Hénon 映射的 Feistel 结构,将混沌映射与该结构溶合在一起,由此设计出基于 Feistel 结构的混沌密码算法,该算法最大的优点是加密的轮次和子密钥的构造是基于混沌系统动态更新的。并从理论和数字实验两方面对其安全性进行了评估、分析。文章第2节简单介绍 Feistel 结构的基本思想和原理;第3、4节分别详述 Hénon 映射的密码学特性和算法设计过程;第5节对算法的安全性进行分析,包括密钥空间、混乱和扩散特性等;最后对论文进行总结。

2 Feistel 结构

分组密码是一种在密钥控制下的变换,该变换将一个固定长度的明文(密文)分组转换成一个密文(明文)分组。由于其具有速度快、易于标准化和便于软硬件实现等特点,通常是信息与网络安全中实现数据加密、数字签名、认证及密钥管理的核心体制,如 DES、RC5、FEAL、GOST、LOKI 等,采用的都是分组密码算法。在这些分组密码都采用了一种叫做 Feistel 的结构[10,11],Feistel 结构把任何函数都转化为一种转换,是一种典型的迭代结构,也是一种乘积形式的密码变换。它能够充分实现扩散与混乱,构成强度很高的密码系统。用数学表达式来表达,其第 i 轮的加密变换为:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases} \tag{1}$$

其中,$\oplus$ 表示按位异或,F 是轮函数,K_i 是第 i 轮的子密钥,L_i 和 R_i 分别是密文的左半部分和右半部分。

式(1)所描述的是左右长度相同的"平衡 Feistel 结构",在加密时,算法将长度为 $2n$ 比特的明文分组 m 分为两个长为 n 比特的部分 L_0 和 R_0,即 $m=L_0R_0$,每轮只对 R_0 进行加密。如 DES 就是采用的这种结构,考虑加密过程中的扩展置换,DES 中需同时处理的长度是48比特。而文[4]采用的是左右长度不同的"非平衡 Feistel 结构",分组长度同样为64比特,但需同时处理的长度却是64比特。我们知道明文分组长度越大,敌手破译的难度也越大,但计算机能够处理的字的长度却是有限的,又迫使分组的长度不能太长。可见,Feistel 结构是影响分组密码算法中分组长度的一个重要因素,制约着分组密码算

法的安全性和运行速度。本文设计了一种动态的 Feistel 结构，加密的轮数不像 DES 算法或者 HOST 算法那样固定的16轮或32轮，并且子密钥随着混沌系统和密文动态更新。

3 混沌系统及其特性分析

人类对混沌现象的认识，是非线性科学最重要的成就之一。经过比较深入的研究，人们发现一个混沌动力学系统的演化具有对初值高度敏感性、伪随机的轨道具有不可预测性、在信息传输过程中呈现连续宽带功率谱的特点。这些特性与密码学中对轮函数、伪随机序列发生器、长周期密钥等的要求非常近似，也正是由于二者有如此多的相似之处，近十年来，混沌动力学系统在通信、密码学中的应用才引起了人们广泛的注意，已发展成为一个非常活跃的研究领域。

本文应用混沌理论中非常经典的 Hénon 映射作为加密变换的轮函数，主要是基于两个方面的原因：一是理论上对其混沌行为的研究比较深入，二是它具有很好的密码学特性。

在非线性研究领域，对 Hénon 映射的混沌特性的研究比较深入，有兴趣的读者请看文[7,9]。对 Hénon 映射：

$$\begin{cases} x_{n+1}=1-px_n^2+y_n \\ y_{n+1}=qx_n \end{cases} \tag{2}$$

它是一个二维的非线性混沌系统，当1.050<p<1.085，q=0.3时，系统产生混沌现象。当 q=0.3，1.050<p<1.085时的部分分岔图及 q=0.3，p=1.4，迭代4000次的“银河”状奇怪吸引子如图1所示。该系统具有很多优良特性。本文只对其混沌行为和密码学特性进行分析。下面我们对它的密码学特性进行定性分析。

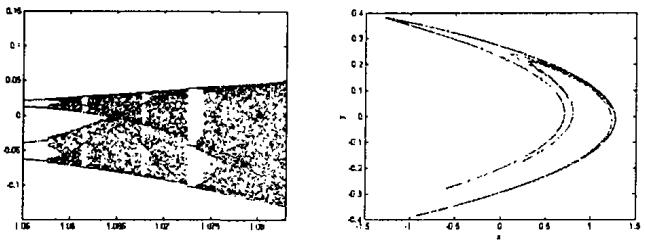

图1 Hénon 映射的分岔图和奇怪吸引子

1)Hénon 映射一大特点是对初始值有极其敏感的依赖性。将其对初值的敏感性充分体现在加密算法对明文和密钥的扩散性与混乱性上，只要算法在初值或明文上有很小的改动，所得到的密文就“面目全非”。混沌映射这一特性很适合于分组密码系统的密钥流生成函数。图2是初值分别取 x_0=0.2345、y_0=0.1234和 x_0=0.2346、y_0=0.1235时迭代100次的 x 轨道图。

2)Hénon 映射具有优良的伪随机性，其轨道的演化是非周期、不收敛的，具有很好的随机性及不可预测性。我们取初值 x=0.20，y=0.10(作为密钥 k 的一部分)，对映射进行迭代。取序列长度 N=5000，相关间隔 M=1000，对其混沌实值序列按如下公式计算相关函数 $R_x(m)$：

$$R_x(m)=\begin{cases} \dfrac{1}{N-m}\sum_{n=1}^{N-m}X_nY_{n+m} & m=0,1,\cdots,M \\ \dfrac{1}{N-|m|}\sum_{n=|m|}^{N}X_nX_{n+m} & m=-1,-2,\cdots,-M \end{cases} \tag{3}$$

当取 $Y=X$ 时，其非周期自相关如图3，改变初值为 x_0=0.2001，y=0.1001时两个混沌序列的互相关特性如图4。可见其具有很好的密码学所需要的相关特性。

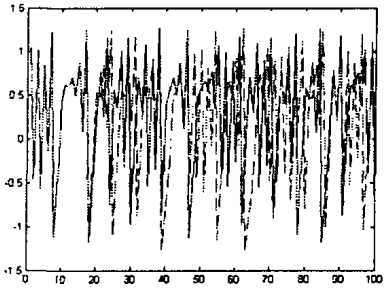

图2 混沌轨道对初值敏感性

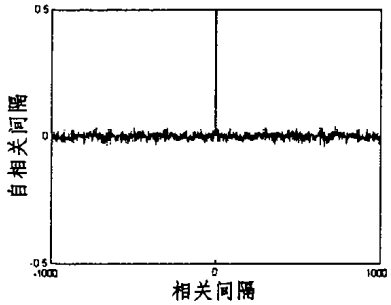

图3 自相关特性

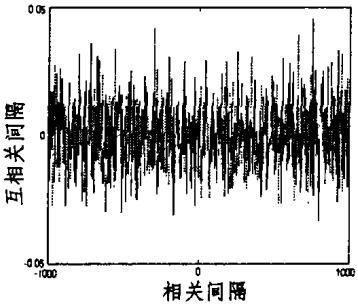

图4 互相关特性

为便于 Feistel 结构的设计及软件实现，我们将 Hénon 映射写为：

$$x_{n+1}=bx_{n-1}+1-ax_n^2=F(x_{n-1},x_n,z_{n-1}) \tag{4}$$

4 算法设计

本文采取如下的分组密码模式：以32位分组对数据加密，32位一组的明文从算法的一端输入，32位密文从另一端输出。密钥的长度是64位。假设明文为 $P=P_1P_2\cdots P_m$，对应的密文为 $C=C_1C_2\cdots C_m$，这里 m 是分组个数。密钥为 $K=K_1K_2\cdots K_n$，n=9。

4.1 基于 Hénon 映射的 Feistel 结构设计

图5为 Feistel 结构图，也就是一轮加密变换的轮函数。图中，L_{i-1}和 R_{i-1}分别表示当轮密文 C_{i-1}的左半部分和右半部分。函数 G 是利用 Hénon 映射产生的子密钥 Z_i，其过程描述如下：

步骤1：根据以下公式(4)、(5)计算 X_i、N_i：

$$X_i=(K_1\oplus K_2\oplus\cdots\oplus K_n)/256 \tag{5}$$

$$N_i=(K_1+K_2+\cdots K_n)\bmod 256 \tag{6}$$

步骤2：计算混沌系统式(4)的初始值 X 和混沌迭代次数 X：

$$X=(X_i+R_{i-1}/65536)\bmod 1,N=floor(N_i+X*256)$$

步骤3：用 X 作为 Hénon 映射的初始值，迭代 N 次最后得到 X_N。

步骤4:计算子密钥:$Z_i=(floor(R_{-1}\times X_N)\bmod 8)+1$。

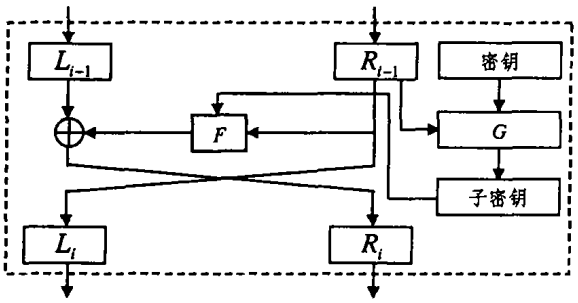

图5 基于 Hénon 映射的 Feistel 结构图

Feistel 结构中我们选用 GOST 算法[8]中的 S 盒作为的 F 函数,如表1所示。子密钥 Z_i 为 S 盒的中输入的序号,在 GOST 中使用了8个不同的 S 盒,每个 S 盒是数0到15的一个置换,例如 S 盒1定义为:4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3,在这种情况下,如果 S 盒输入为0,输出为4;输入为1则输出为10,其他以此类推。

表1 GOST 算法的 S 盒

S-盒1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S-盒2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S-盒3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S-盒4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S-盒5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S-盒6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S-盒7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S-盒8	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

4.2 算法详细描述

基于 Hénon 映射和 Feistel 结构的分组密码算法具体描述如下:

步骤1:假设 P_k 是第 k 个明文分组,那么应用 Feistel 结构对当前明文加密 P_k 次,然后输出对应的密文分组 C_k。如果 k 等于1,那么 R_k 等与32;如果 k 大于1,那么 R_k 通过以下方法计算 R_k 的值。

(1)假设 L^*_{k-1},R^*_{k-1}表示第 $k-1$ 个密文分组的左半部分和右半部分,长度为16bit;同时假设 $L^*_{k-1,h}$,$L^*_{k-1,l}$为 L^*_{k-1}的高8位和低8位,同理,$R^*_{k-1,h}$,$R^*_{k-1,l}$为 R^*_{k-1}的高8位和低8位。

(2)计算下列值:

$T^*_{k-1}=(L^*_{k-1}\oplus R^*_{k-1})/65536$

$X^*_S=T^*_{k-1}\bmod l$

$N^*_S=L^*_{k-1,h}\oplus L^*_{k-1,l}\oplus R^*_{k-1,h}\oplus R^*_{k-1,l}$

$X^*_N=L(X^*_i,N^*_i)$

X^*_N 表示用 X^*_i 作为 Hénon 映射的初始值,迭代 N^*_i 次最后得到的结果。

(3)计算 R_k,$R_k=16+floor(X^*_N\times 16)$。

步骤2:重复步骤1,直到所有的明文都被加密。

解密过程与加密过程相似。

5 模拟仿真及分析

测试算法的性能,我们用两个不同类型、不同大小的文件进行加密然后解密实验,记录下有关的数据,并与另外两个相似的混沌加密算法进行比较。实验环境为:PIV 2.4GHZ,内存为256M,硬盘为80G 的个人计算机,所用到的两个文件是:

文件1:图像文件(Lenna.bmp,图6),大小为134kB;

文件2:Word 文件(.DOC),大小为560kB。

所使用的三种算法分别为 Baptista(算法一)和 Wong(算法二)所提出的混沌加密算法及本文所描述的算法(算法三)。所有文件及算法都能顺利完成加密与解密,但所需要的时间与密文的分布等相关特性却相差很大。

5.1 加密时间分析

针对两个文件运用三种算法的加密结果的部分数据见表2。从表中可以看出,本文所提算法最快,其次是 Wong 的算法,而 Baptista 的算法运行速度太慢,不适合于加密现在广泛的多媒体文件,更不适于在 Internet 网上运行。

表2 运用三种算法对两个不同的文件加密后的部分统计数据

	算法一		算法二		算法三	
	File 1	File 2	File 1	File 2	File 1	File 2
加密时间(秒)	13.4	47.8	4.8	11.39	0.89	2.89
密文大小(KB)	286	1120	286	1120	134	560

5.2 密文大小比较

从表2还可以看出,三种算法所得到的密文大小也不一样,前两种算法所得到的密文大小相同,这是因为它们加密一个1字节(8 bits)的字符,其密文都是混沌系统的迭代次数,数据将达到几万次,需要用2个字节(16 bits)来表示,所以其密文长度最少是明文的两倍。如果用这两种算法来加密一个多媒体文件(长度通常为几兆),其密文文件大小将达到十几兆,甚至几十兆,这是不可容忍的。而本文所取算法其密文文件长度几乎与明文相同,只是在明文长度不是32 bits 的倍数时,密文要比明文长几个字(最多7个字符)。

5.3 密文分布分析

密文分布是一个密码系统最重要的特性之一,它将直接影响到密码系统的安全。一个分布不均匀密文,往往是密码分析者进行唯密文攻击的首选入口[17]。为更清晰地描述这一特性,我们用图像的直方图来表达。从图6~11可以看出,本文所提算法所得到的密文在整个密文空间的分布都非常均匀。

通过计算三种算法所得密文的标准差,我们也可以很明显地看出其密文分布的偏离情况。计算公式为:

$$STD=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(c_i-\bar{c})^2} \tag{7}$$

三种算法的计算结果分别为2569.13、622.67和71.31,可见算法一的分散程度最大,算法二次之,而本文所提算法最小,与算法一相差35倍。

图6 明文图

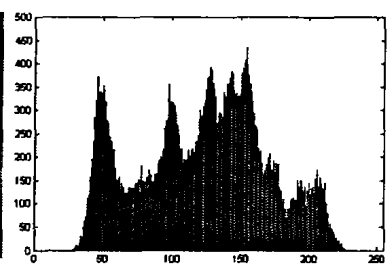

图7 明文字符分布图

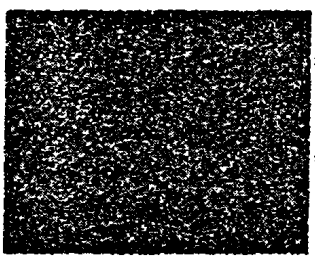

图8 密文

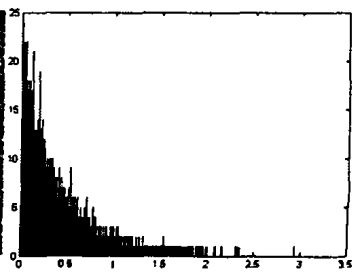

图9 算法一的密文分布

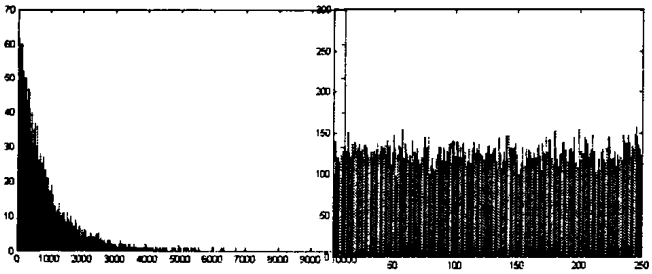

图10 算法二的密文分布　　图11 算法三的密文分布

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。通过混论和扩散，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 Jridrich J. Image Encrytion 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]. Massachuselts 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 servce 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