第 42 卷 第 9 期 计 算 机 工 程 2016 年 9 月
Vol. 42 No. 9 Computer Engineering September 2016

·移动互联与通信技术· 文章编号：1000-3428(2016)09-0089-05 文献标志码：A 中图分类号：TN973

基于差分进化狼群算法的 GNSS 欺骗干扰检测

孙闽红，邵章义，秦 源，闫云珍

（杭州电子科技大学 通信工程学院，杭州 310018）

摘 要： 针对狼群算法（WPA）收敛速度慢且易陷入局部最优解的问题，提出一种差分进化狼群算法（DE-WPA）并将其应用于全球导航卫星系统欺骗干扰检测中。将非线性干扰机/卫星发射机和无线信道综合建模为 Hammerstein 模型，通过 DE-WPA 辨识该模型参数并以模型参数为特征向量进行欺骗干扰检测。仿真结果验证了 DE-WPA 在 Hammerstein 模型系统辨识上的有效性，而且相对于最小二乘估计法、经典迭代法和基本 WPA 算法，DE-WPA 算法具有更高的模型参数辨识精度和欺骗干扰识别率。

关键词： 全球导航卫星系统；欺骗干扰；系统辨识；Hammerstein 模型；狼群算法；差分进化

中文引用格式： 孙闽红，邵章义，秦 源，等. 基于差分进化狼群算法的 GNSS 欺骗干扰检测[J]. 计算机工程，2016，42(9)：89-93.

英文引用格式： Sun Minhong，Shao Zhangyi，Qin Yuan，et al. GNSS Spoofing Jamming Detection Based on Differential Evolution-Wolf Pack Algorithm[J]. Computer Engineering，2016，42(9)：89-93.

GNSS Spoofing Jamming Detection Based on Differential Evolution-Wolf Pack Algorithm

SUN Minhong，SHAO Zhangyi，QIN Yuan，YAN Yunzhen

（School of Communication Engineering，Hangzhou Dianzi University，Hangzhou 310018，China）

【Abstract】 Since the Wolf Pack Algorithm（WPA） has some demerits，such as slow convergence and being easy to trap in local optimum，a Differential Evolution-Wolf Pack Algorithm（DE-WPA） is proposed and applied in spoofing jamming detection for Global Navigation Statellite System（GNSS）. A Hammerstein model is applied to establish the model of the nonliner jammer or the satellite transmitter and the wireless channel at first. Then the DE-WPA is utilized to estimate parameters of the model. Next，a method is employed to identify the spoofing jamming with the estimated model parameters. Simulation results show that the DE-WPA is effective for the Hammerstein model system identification. It can obtain higher model parameter identification precision and deception jamming recognition rate than the Least Square（LS） estimation algorithm，the iterative algorithm and WPA algorithm.

【Key words】 Global Navigation Satellite System（GNSS）；spoofing jamming；system identification；Hammerstein model；Wolf Pack Algorithm（WPA）；Differential Evolution（DE）

DOI： 10.3969/j.issn.1000-3428.2016.09.016

1 概述

全球导航卫星系统（Global Navigation Satellite System，GNSS）[1]极易受到多种形式的干扰，其中主要的干扰样式之一为欺骗干扰[2]。该类干扰具有与真实信号相类似的增益，并在时、频、空等多域与真实信号完全或者部分重叠，对其识别的效果通常不太理想。

现有研究主要基于干扰信号与真实信号在某个参数上的差异进行识别，如绝对功率[3]、到达时间[4]、到达角[5]等。近年来，对发射机建模并基于模型参数来识别无线发射机取得了一些进展[6-7]，其研究表明基于模型参数的识别方法即使在样本数不多、信噪比（Signal to Noise Ratio，SNR）较低时也有效。然而这些估计模型参数的方法大都为最小二乘（Least Square，LS）估计法和迭代法，存在辨识精度低或收敛性不能被严格证明的不足，而智能算法可以较好地解决上述问题。2013 年，吴虎胜等人提出

基金项目： 国家自然科学基金资助项目（61271214，61471152）；浙江省自然科学基金资助项目（LZ14F010003）。

作者简介： 孙闽红（1974－），男，副教授、博士，主研方向为信号处理；邵章义、秦 源、闫云珍，硕士。

收稿日期： 2015-09-02 **修回日期：** 2015-10-08 **E-mail：** szy0900301213@163.com

狼群算法(Wolf Pack Algorithm,WPA)[8]并证明该算法以概率 1 收敛于问题的最优解,但狼群算法有收敛速度慢、易陷入局部最优、局部搜索能力不强等缺点[9]。因此,本文提出一种差分进化狼群算法(Differential Evolution-Wolf Pack Algorithm,DE-WPA)。该算法在 WPA 算法的全局收敛性基础上,引入差分进化算法[10-12](Differential Evolution,DE)的差分变异,使算法能跳出局部最优解,提高全局搜索能力。此外,该算法还能发挥差分进化算法在局部搜索方面的优点。为验证 DE-WPA 的优越性,将其应用于卫星导航欺骗干扰识别。综合考虑发射机和干扰机的非线性特性及无线信道的多径效应,将整个通信系统[13]等效为 Hammerstein 模型,利用 DE-WPA 进行系统辨识,以此进行欺骗干扰识别,并与基本 WPA、经典最小二乘估计法和迭代法进行性能比较。

2 系统建模

以全球定位系统(Global Positioning System,GPS)为例,发射机结构如图 1 所示。

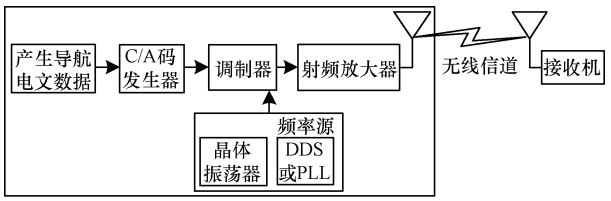


图 1 GPS 发射机结构

由于发射机和干扰机的系统组成相同,因此采用相同方法进行建模,为论述方便只对发射机建模进行讨论。在发射机建模过程中,发射机可用一个无记忆非线性多项式模型表示[14]。由于偶次项会被射频滤波器滤除,因此仅考虑奇次项,如式(1)所示。

$$\begin{aligned} f(d(n)) &= b_1 d(n) + b_3 d(n)\,|d(n)|^2 \\ &\quad + b_5 d(n)\,|d(n)|^4 + \cdots + b_{2m-1} d(n)\,|d(n)|^{2m-2} \\ &= \sum_{i=1}^{M} b_{2i-1} d(n)\,|d(n)|^{2i-2} \end{aligned} \tag{1}$$

其中,M 是多项式系数的个数;$d(n)$ 是输入信号;b_k 是多项式系数。另外,在不改变系统特性的情况下,为确定系统的唯一性,令 $b_1 = 1$。

对于图 1 的无线频率选择性信道可以用一个线性时不变子系统[6]进行表述,信道可以建模为一个有限脉冲响应(Finite Impulse Response,FIR)滤波器,信道输入输出关系为:

$$y(n) = \sum_{k=0}^{N-1} h_k x(n-k) + w(n) \tag{2}$$

其中,h_k 是信道响应系数;N 是 FIR 滤波器的阶数;$w(n) \sim N(0,\sigma^2)$ 是加性高斯白噪声;$y(n)$ 为接收机接收到的信道输出信号。

整个系统的输入输出关系可以表示为:

$$y(n) = \sum_{k=0}^{N-1} h_k \sum_{i=1}^{M} b_{2i-1}\,|d(n-k)|^{2i-2} d(n-k) + w(n) \tag{3}$$

系统辨识理论将式(3)的数学模型称为 Hammerstein 模型[15],即一个线性子系统级联于一个非线性子系统之后。在卫星导航接收机中,可估计得到发射端的数据,即模型中的输入和输出数据对接收机而言均为已知,所以,对模型参数进行辨识是可行的。

3 基本狼群算法

狼群算法模拟了狼群的协作捕猎行为,具有较好的全局收敛性和计算鲁棒性。在 WPA 中,狼群中分为头狼、探狼以及猛狼。头狼是具有最优目标函数的人工狼,指挥整个狼群的行动。探狼是较少的具有较优目标函数值的人工狼,在猎物的可能活动范围中进行游猎。猛狼只参与最后对猎物的围攻行为。每个猎物源表示为优化问题的一个可行解,猎物源的气味浓度代表相应解的适应度或优化问题的目标函数值。算法具体步骤如下[8]:

步骤 1 初始化。初始化狼群中人工狼位置 X_i,种群规模 N,最大迭代次数 $k_{\max}$,探狼比例因子 α,最大游走次数 $T_{\max}$,距离判定因子 w,步长因子 S,更新比例因子 β。

步骤 2 选取最优人工狼为头狼,除头狼外最佳的 S_num 匹人工狼为探狼并执行游走行为,直到某只探狼侦察到的猎物气味浓度 Y_i 小于头狼所感知的猎物气味浓度 Y_{lead} 或达到最大游走次数 $T_{\max}$,则转步骤 3。

步骤 3 人工猛狼根据式(4)向猎物奔袭,若途中猛狼感知的猎物气味浓度 $Y_i < Y_{\text{lead}}$,则 $Y_{\text{lead}} = Y_i$,替代头狼并发起召唤行为;若 $Y_i \geqslant Y_{\text{lead}}$,则人工猛狼继续奔袭直到 $d_{is} < d_{\text{near}}$,转步骤 4。

$$x_{id}^{k+1} = x_{id}^{k} + step_b^d (g_d^k - x_{id}^k) / |g_d^k - x_{id}^k| \tag{4}$$

步骤 4 探狼联合猛狼按式(5)以头狼所在位置为中心,执行围攻行为。

$$x_{id}^{k+1} = x_{id}^{k} + \lambda \cdot step_c^d \cdot |G_d^k - x_{id}^k| \tag{5}$$

步骤 5 按胜者为王的头狼产生规则对头狼位置进行更新,然后根据强者生存的狼群更新机制进行群体更新。

步骤 6 判断是否满足精度要求或达到最大迭代次数 $T_{\max}$,若达到则输出头狼的位置,即待优化问题的最优解;否则转步骤 2。

4 差分进化狼群算法

狼群算法在寻优到一定阶段后,尤其是在后期,

部分人工狼在局部极值附近聚集,从而导致寻优进展缓慢,难以跳出局部最优。因此,本文引入差分进化算法的差分策略,通过该算法中的变异、交叉和选择过程,使得算法能跳出局部最优,同时充分利用差分进化算法在局部寻优方面的优点,提高算法的寻优精度。

DE-WPA 算法流程如图 2 所示。该算法的基本思想是:种群先按照基本狼群算法依次执行游走、奔袭、围攻行为,再进行差分进化(即变异、交叉及贪婪选择操作)及更新头狼位置,并根据强者生存的狼群更新机制进行群体更新。总体上,该算法依次进行 WPA 算法搜索和 DE 算法变异,是一种 2 层的串行结构。

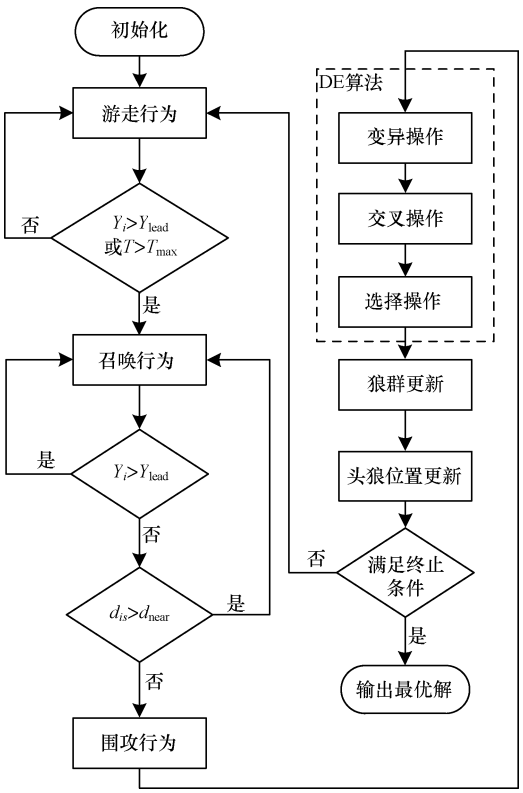


图 2　DE-WPA 算法流程

5　基于系统辨识的欺骗干扰识别

系统辨识的目的是在给定系统输入 $u(k)$ 和系统输出 $y(k)$ 的基础上,基于某种准则建立目标函数,求解该目标函数得到系统模型参数向量的估计 $\hat{\boldsymbol{\theta}}$。本文采用最小均方误差准则,以实际模型的输出与参数模型输出的均方误差(Mean Square Error, MSE)作为辨识 Hammerstein 模型的目标函数,即:

$$f(\hat{\boldsymbol{\theta}}) = \frac{1}{s}\sum_{i=1}^{s} | y(k-i) - \hat{y}(k-i) |^2 \tag{6}$$

其中,s 为信号长度;$\hat{y}(k)$ 为估计参数模型的输出。至此,非线性系统辨识问题就转化为参数空间上的最小值问题,通过 DE-WPA 算法对式(6)求最小值并估计出与之对应的模型参数值。

设卫星导航发射机与干扰机及其无线信道的模型参数向量分别为 $\boldsymbol{\theta}_1$ 和 $\boldsymbol{\theta}_2$。为了量化评价系统模型参数的相似性,引入余弦相似度,其定义如下:

$$\cos\alpha = (\boldsymbol{\theta}_1^{\mathrm{H}}\boldsymbol{\theta}_2) / | \boldsymbol{\theta}_1 \| \boldsymbol{\theta}_2 | \tag{7}$$

在利用 DE-WPA 算法获得系统参数的估计值之后,采用较直观的欧氏距离比较法进行识别,判决准则为:

$$| \hat{\boldsymbol{\theta}} - \boldsymbol{\theta}_1 | \underset{H_1}{\overset{H_0}{\gtrless}} | \hat{\boldsymbol{\theta}} - \boldsymbol{\theta}_2 | \tag{8}$$

其中,H_0 表示接收机接收到欺骗干扰信号;H_1 表示接收机接收到真实信号。

6　仿真实验与结果分析

假设欺骗干扰为转发式干扰,为了验证 DE-WPA 在识别欺骗干扰上的效果,仿真产生 GPS 的 C/A 码信号,调制方式采用四相相移键控(Quadrature Phase Shift Keyin,QPSK)调制。设式(3)的模型参数向量为:$\boldsymbol{\theta} = [b_1 \quad b_3 \quad b_5 \quad b_7 \quad h_1 \quad h_2 \quad h_3]$,其中,非线性模块阶数为 7;线性模块阶数为 3。具体参数值见表 1。

表 1　实际参数设置

类别	非线性子系统参数 b				线性子系统参数 h		
	b_1	b_3	b_5	b_7	h_1	h_2	h_3
发射机	1	-0.013 5	-0.008 6	-0.001 7	0.990 6	0.062 8	0.007 9
干扰机	1	-0.018 7	-0.005 3	-0.002 9	0.972 3	0.096 3	0.019 4

计算两者余弦相似度为 0.999 3,对应的两向量夹角为 1.086 1°,表明真实卫星信号与欺骗干扰信号非常相似。

为充分验证 DE-WPA 在系统辨识及欺骗干扰识别中的性能,本文将其与系统辨识中的经典迭代法、最小二乘估计法、狼群算法进行仿真性能比较。SNR 设为 2 dB ~ 26 dB,步长为 4 dB,在不同 SNR 下每种算法分别进行 2 000 次独立实验。除了最小二乘估计法是一次性估计完成,其余算法最大迭代次数为 300 次,狼群种群规模为 50。WPA 的主要参数

设置为:$\alpha=3$,$T_{max}=20$,$w=100$,$S=300$,$\beta=2$;DE-WPA 的主要参数设置为:$\alpha=4$,$T_{max}=20$,$w=100$,$S=300$,$\beta=2$,交叉概率 $P_{cross}=0.9$,缩放因子 $F=0.6$。

首先比较各算法的时间复杂度,通过平均运行时间来衡量。表 2 给出了 4 种算法每次估计的平均运行时间。可以看出,传统算法要比智能算法快很多,特别是最小二乘估计法由于是直接估计无需迭代,因此运行速度非常快;而智能算法由于每一次循环过程中又包含多个个体的多次智能行为,因此运行时间更长。在 2 种智能算法中,DE-WPA 算法由于加入了 DE 算法的操作,所以,运行时间比 WPA 要稍长。

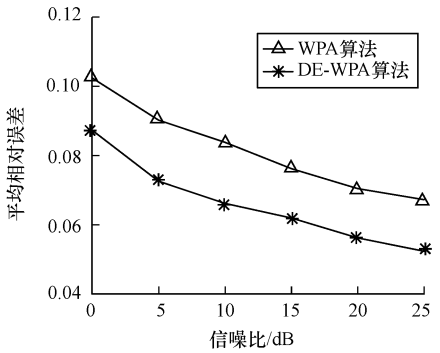
表 2 算法平均运行时间 s

算法	平均运行时间
DE-WPA	503.24
WPA	324.43
经典迭代法	78.21
最小二乘估计法	0.37

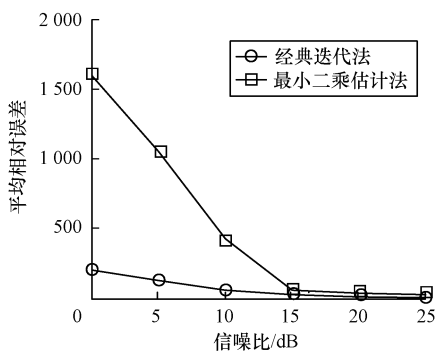
其次为了评价系统辨识的效果,定义平均相对误差(Average Relative Error,ARE):

$$ARE=0.5\times(|E(\hat{\boldsymbol{\theta}}_1)-\boldsymbol{\theta}_1|/|\boldsymbol{\theta}_1|+|E(\hat{\boldsymbol{\theta}}_2)-\boldsymbol{\theta}_2|/|\boldsymbol{\theta}_2|) \tag{9}$$

其中,$E(\hat{\boldsymbol{\theta}})$表示对多次估计值取均值。根据式(9)计算得到各算法的 ARE 随 SNR 变化,如图 3 所示。



(a)WPA与DE-WPA算法



(b)经典迭代法与最小二乘估计法

图 3 平均相对误差随信噪比的变化曲线

由图 3 可以看出,4 种算法的 ARE 都随着 SNR 的增大而减小,即噪声越小,估计值越准确。同时,2 种智能算法的 ARE 要远小于传统辨识方法的 ARE。这是由于经典最小二乘估计法和迭代法对噪声特别敏感,所估计的参数值与真实值相差几个数量级,因此其平均相对误差较大。对于 2 种智能算法,DE-WPA 的 ARE 均小于 WPA 的 ARE,在 2 dB ~ 26 dB 范围内平均相差 0.015 6。

最后比较 4 种算法的识别率,如图 4 所示。由图 4 可知,DE-WPA 和基本 WPA 的识别率都随着 SNR 的变大而变大。对于两者而言,若要达到识别率为 90%,DE-WPA 的 SNR 比 WPA 要高出近 4 dB,并且 DE-WPA 的识别率平均比 WPA 要高 5.11%。而经典迭代法和最小二乘估计法由于对噪声特别敏感,参数辨识值来回跳变,因此识别率在 50% 随机波动,即这 2 种方法在此失效。

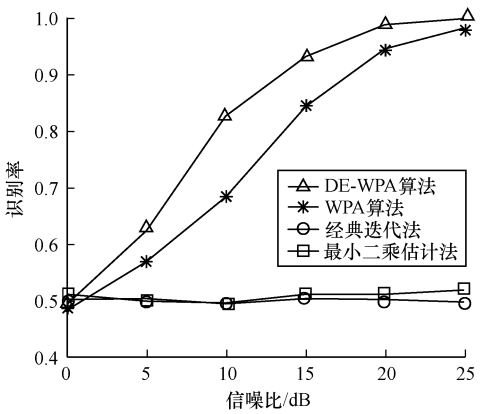


图 4 识别率随信噪比的变化曲线

以上实验结果表明,本文所提出的 DE-WPA 算法虽然时间复杂度略高于 WPA 算法,但是其平均相对误差和识别率均优于 WPA 算法。

7 结束语

本文提出一种基于差分进化的改进狼群算法,并将其应用于卫星导航欺骗干扰的识别中。通过在基本的 WPA 算法中引入差分进化策略,从而达到跳出局部最优解以及提高算法的寻优精度等目的。为验证算法性能,将其与最小二乘估计法、迭代法以及基本 WPA 算法进行对比。实验结果表明,DE-WPA 算法在 ARE 上比 WPA 算法平均低 0.015 6,在识别率上比 WPA 平均高出 5.11%,因此,DE-WPA 算法在系统辨识及干扰识别中更具优越性。由于加入了差分进化策略,DE-WPA 算法的时间复杂度略高,因此下一步研究将在不影响算法识别性能的前提下对其进行优化。

参考文献

[1] Kaplan E D, Hegarty C J. Understanding GPS Principles and Applications[M]. 2nd ed. Boston, USA: Artech House, 2006.

[2] Basker S. Jamming: A Clear and Present Danger[J]. GPS World, 2010, 21(4): 8-9.

[3] Nielsen J, Broum A, Lachapelle G. Spoofing Detection and Mitigation with a Moving Handheld Receiver[J]. GPS World, 2010, 21(9): 27-33.

[4] Humphreys T E, Ledvina B M, Psiaki M L, et al. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer[C]//Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation. Anaheim, USA: [s. n.], 2008: 2314-2325.

[5] Montgomery P Y, Humphreys T E, Ledvina B M. Receiver-autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer[C]//Proceedings of 2009 International Technical Meeting of the Institute of Navigation. Anaheim, USA: [s. n.], 2009: 124-130.

[6] Liu Mingwei, Doherty J F. Nonlinearity Estimation for Specific Emitter Identification in Multipath Channels[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 1076-1085.

[7] Polak A C, Dolatshahi S, Goeckel D L. Identifying Wireless Users via Transmitter Imperfections[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(7): 1469-1479.

[8] 吴虎胜,张凤鸣,吴庐山. 一种新的群体智能算法——狼群算法[J]. 系统工程与电子技术,2013,35(11):2430-2438.

[9] 李国亮,魏振华,徐　蕾. 基于改进搜索策略的狼群算法[J]. 计算机应用,2015,35(6):1633-1636,1687.

[10] Storn R, Price K. Differential Evolution——A Simple and Efficient Adaptive Scheme for Global Optimization over Continuous Spaces[J]. Journal of Global Optimization, 1997, 11(4): 341-359.

[11] 杨启文,蔡　亮,薛云灿. 差分进化综述[J]. 模式识别与人工智能,2008,21(4):506-511.

[12] 张大斌,杨添柔,温　梅,等. 基于差分进化的鱼群算法及其函数优化应用[J]. 计算机工程,2013,39(5):18-22,27.

[13] 沈　超,裘正定. 基于 MatLab/Simulink 的 GPS 系统仿真[J]. 系统仿真学报,2006,18(7):1857-1860,1889.

[14] Barradas F M, Cunha T R, Lavrador P M, et al. Polynomials and LUTs in PA Behavioral Modeling: A Fair Theoretical Comparison[J]. IEEE Transactions on Microwave Theory and Techniques, 2014, 62(12): 3274-3285.

[15] Xia Hong, Sheng Chen, Yu Gong, et al. Nonlinear Equalization of Hammerstein OFDM Systems[J]. IEEE Transactions on Signal Processing, 2014, 62(21): 5629-5639.

编辑　陆燕菲

(上接第 88 页)

[10] Gou Liang, Zhang Gengxin, Bian Dongming, et al. Relay Scheme Based on Distributed Luby Transform Codes for InterPlaNetary Internet[J]. China Communications, 2013, 10(10): 1-11.

[11] Ying Huang, Jing Lei. Fountain Codes Design for Asynchronous Multi-relay System[C]//Proceedings of the 3rd International Conference on Computer Science and Network Technology. Washington D. C., USA: IEEE Press, 2013: 752-756.

[12] Luby M. LT Codes[C]//Proceedigns of the 43rd Annual IEEE Symposium on Foundations of Computer Science. Washington D. C., USA: IEEE Press, 2002: 271-282.

[13] Shokrollahi A. Raptor Codes[J]. IEEE Transactions on Information, 2006, 52(6): 2551-2567.

[14] Bogino M, Cataldi P, Grangetto M, et al. Sliding-window Digital Fountain Codes for Streaming of Multimedia Contents[C]//Proceedings of IEEE International Symposium on Circuits and Systems. Washington D. C., USA: IEEE Press, 2007: 3467-3470.

[15] Zhao Danfeng, Qian Jinxi, Wu Yuping. The Design of Variable Frame Length LT Code Based on Limiting Conditions[C]//Proceedings of the 2nd International Conference on Future Computer and Communication. Washington D. C., USA: IEEE Press, 2010: 787-790.

[16] Rahnavard N, Vellambi B N, Fekri F. Rateless Codes with Unequal Error Protection Property[J]. IEEE Transactions on Information Theory, 2007, 53(4): 1521-1532.

[17] Ahmad S, Hamzaoui R, Al-Akaidi M. Unequal Error Protection Using LT Codes and Block Duplication[C]//Proceedings of Middle Eastern Multi Conference on Simulation and Modeling. Tucson, USA: [s. n.], 2008: 1959-1964.

[18] Sejdinovic D, Vukobratovic D, Doufexi A, et al. Expanding Window Fountain Codes for Unequal Error Protection[J]. IEEE Transactions on Communications, 2009, 57(9): 1020-1024.

[19] Luby M, Mitzenmacher M, Shokrollahi A. Analysis of Random Processes via Or-And Tree Evaluation[C]//Proceedings of the 9th SIAM Symposium on Discrete Algorithms. San Francisco, USA: SIAM, 1998: 364-373.

[20] Li Luying, Li Zongyan, Wang Wenbo. Adaptive Iteration for Fountain Decoding[J]. The Journal of China Universities of Posts and Telecommunications, 2010, 17(2): 22-25.

编辑　金胡考