基于构造代价函数求解的自同步扰码盲识别方法

韩树楠* 张 旻 李歆昊
(国防科技大学电子对抗学院 合肥 230031)

摘 要：由于卷积码序列的 0,1 bit 的概率几乎均衡，对于卷积码自同步加扰的扰码盲识别，现有的基于输入序列 0, 1 bit 概率不均衡性的识别方法均已失效，为此该文提出一种新的自同步扰码盲识别方法。首先将卷积码自同步加扰序列进行分块处理，通过加扰数据块与卷积码校验向量相乘产生新的序列；然后以最大化新生成序列间线性约束关系成立概率为准则，利用解调输出的软判决序列建立自同步扰码反馈多项式系数的代价函数；最后根据自同步扰码反馈多项式的项数特点，在求解代价函数时改进了动态搜索烟花算法，增加了对烟花个体元素值的约束操作，由求解出的参量值识别出自同步扰码反馈多项式。仿真实验验证了所提方法的有效性，该方法无需遍历搜索反馈多项式，且具有较好的鲁棒性，所需数据量小，随着数据量的增大和扰码阶数的降低，其识别正确率逐渐提高。

关键词：自同步扰码；卷积码；反馈多项式；校验向量；烟花算法
中图分类号：TN919 **文献标识码**：A **文章编号**：1009-5896(2018)08-1971-07
DOI: 10.11999/JEIT171026

A Blind Identification Method of Self-synchronous Scramblers Based on Optimization of Established Cost Function

HAN Shunan ZHANG Min LI Xinhao
(*College of Electronic Engineering, National University of Defense Technology, Hefei* 230031, *China*)

Abstract: Since the probability bias between 0 and 1 bit in a convolutional code sequence is very small, the existing method based on the probability bias in the input sequence is ineffective for the identification of a self-synchronous scrambler placed after a convolutional encoder. To solve this problem, a novel method for the blind identification of a self-synchronous scrambler is proposed. First, the scrambled convolutional code sequence is divided into blocks, and a new bit sequence is generated, in which each bit is the dot product of a scrambled bit block with a parity check vector of the convolutional code. Second, based on the criteria of maximizing the probability that the linear equations in the generated bits hold, the cost function of the feedback polynomial coefficients of the self-synchronous scrambler is established using the soft decision sequence, which is the output of the demodulator. Third, according to the characteristic of the number of terms in the feedback polynomial, the dynamic fireworks algorithm is modified by constraining the values of elements in fireworks, and the cost function is optimized using the modified dynamic fireworks algorithm. Simulation experiments show the effectiveness of the proposed algorithm. There is no need to search for the feedback polynomial exhaustively in the proposed algorithm. It is robust to the noise and the number of data required is small. Moreover, along with the increase of the number of received data or the decrease of the order of the feedback polynomial, the correct identification ratio of the proposed method increases.

Key words: Self-synchronous scrambler; Convolutional code; Feedback polynomial; Parity check vector; Fireworks algorithm

1 引言

自同步扰码是通信系统的重要组成部分，在深空通信、卫星通信和移动通信中有着广泛的应用[1,2]。采用自同步扰码能够起到随机化传输序列及数据加密的作用，加扰后的序列中不会出现连续的 0 和 1，有利于平坦化调制信号的功率谱及提取定时信息[3,4]。随着自同步扰码在通信系统中的广泛应用，自同步扰码盲识别技术也应运而生。在认知无线电领域，自同步扰码的盲识别已成为智能接收机中的一项重要技术；在信息对抗领域，非合作方要达到信息截获的目的，数据解扰也是必不可少的关

收稿日期：2017-11-02；改回日期：2018-03-23；网络出版：
*通信作者：韩树楠 hsnnong@163.com
基金项目：国家自然科学基金(61602491)
Foundation Item: The National Natural Science Foundation of China (61602491)

键环节，因此自同步扰码的盲识别具有重要的研究意义和价值。

自同步扰码盲识别的目标是利用截获的加扰数据识别出其反馈多项式，近年来该问题引起了国内外研究者的广泛关注。基于输入序列 0,1 bit 概率的不均衡性，研究者们已提出了一些识别方法。如文献[5]提出基于 Walsh-Hadamard 变换(WHT)的识别方法。该方法首先利用加扰序列间的约束关系建立线性方程组；然后基于 WHT 求解该方程组得到反馈多项式的系数向量。基于 WHT 的识别法需已知自同步扰码阶数，且要求输入序列中 0 的概率大于 1 的概率。文献[6]提出基于重码统计的识别方法，该方法首先利用加扰序列的重码分布特性估计扰码阶数；再遍历该阶数下的所有二项式和三项式进行解扰，根据解扰后序列的 0,1 不均衡性判定扰码的反馈多项式。文献[7]提出基于游程统计的自同步扰码阶数估计方法，该方法统计加扰序列的不同长度的游程数量，根据游程分布估计扰码阶数。文献[8]提出基于比特状态统计的识别方法，该方法遍历一定项数的多项式，根据多项式的系数向量相应地抽取加扰序列，当测试多项式与实际的扰码反馈多项式相同时，抽取比特的状态的概率分布出现明显的不均衡性，由此判定反馈多项式。文献[9]提出基于二元假设检验的识别方法，该方法利用假设检验理论遍历检测反馈多项式的倍式，将检测到的倍式间的最大公约式识别为反馈多项式。文献[10]在已知输入序列 0,1 bit 概率有偏性的条件下，利用梯度法最大化扰码序列间线性关系的成立概率，根据求解结果估计出反馈多项式系数向量。上述识别方法要求输入序列中的 0,1 bit 概率具有明显的不均衡性，且需要较大的数据量。当输入序列是信源编码时，0,1 bit 概率的不均衡性往往能够被满足；而当输入序列是纠错编码时，由于其 0,1 bit 概率几乎相等[11]，此时基于输入序列比特不均衡性的识别方法失效。

针对卷积码加扰的扰码盲识别问题，文献[12]提出了基于校验向量的卷积码同步加扰的扰码识别方法，该方法在卷积码校验向量先验已知的条件下，遍历寻找反馈多项式的稀疏倍式，将稀疏倍式间的最大公约式识别为同步扰码反馈多项式。文献[13]改进了文献[12]的方法，提高了非倍式假设下检验统计量的均值，由此降低了检测稀疏倍式的虚警概率。文献[14]基于多重分形谱，提出了线性分组码与线性分组码自同步加扰的编码类型识别方法。文献[15]提出了一种线性分组码自同步加扰的扰码盲识别方法，该方法遍历所有可能的多项式并对接收序列解扰，利用线性分组码与随机序列游程特性的差异判断是否正确解扰，由此识别出自同步扰码反馈多项式。文献[16]提出了基于码重分布距离的线性分组码自同步加扰的识别方法，该方法首先利用加扰序列矩阵秩的特性估计出线性分组码的码长；然后遍历所有可能的多项式并对接收序列解扰，根据线性分组码与随机序列码重分布的差异判断是否正确解扰并确定反馈多项式的识别结果。由上述分析可知，目前纠错码加扰的扰码识别方法中多是采用遍历搜索的方式，且缺乏对卷积码自同步加扰识别的有效方法。

本文提出一种卷积码自同步加扰的扰码盲识别方法。该方法首先将加扰序列块与卷积码校验向量相乘生成新的序列；然后以最大化生成序列间线性关系的成立概率为准则，利用解调输出的软判决序列构建反馈多项式系数的代价函数；最后基于改进的动态搜索烟花算法最小化该代价函数，根据求解出的参量值识别出自同步扰码反馈多项式。

2 问题描述

本文的目的是解决卷积码自同步加扰情况下的扰码识别问题，所针对的通信传输系统如图 1 所示。图中自同步加扰器由线性反馈移位寄存器组成，其结构如图 2 所示。

图 2 中 $c_t, t>0$ 表示卷积码序列；$y_t, t>0$ 表示卷积码自同步加扰序列；$a_j (1 \le j \le p)$ 为反馈多项式系数，且 $a_i \in \mathrm{GF}\ 2$ 。由图 2 可知，卷积码自同步加扰过程为

$$y_t = c_t \oplus a_1 y_{t-1} \oplus a_2 y_{t-2} \oplus \cdots \oplus a_p y_{t-p} \tag{1}$$

自同步扰码的解扰过程是加扰过程的逆过程，可表示为

$$c_t = y_t \oplus a_1 y_{t-1} \oplus a_2 y_{t-2} \oplus \cdots \oplus a_p y_{t-p} \tag{2}$$

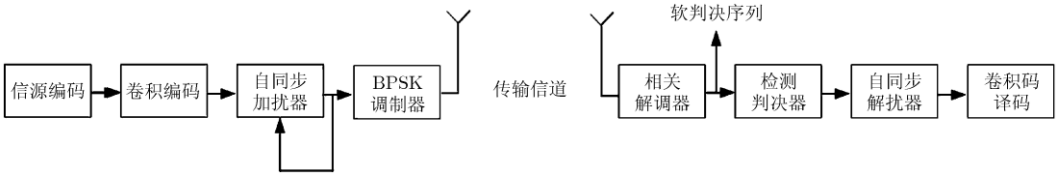

图 1 通信传输系统

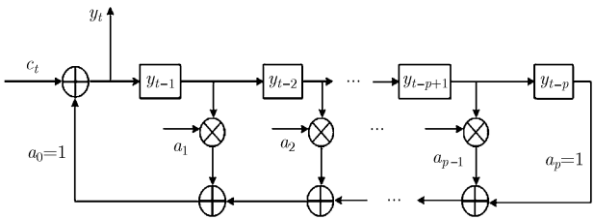

图 2 自同步加扰器结构图

由式(2)可知，若已知反馈多项式 $f(x)=1+a_1x+a_2x^2+\cdots+a_px^p$，则由连续的 $p+1$ 个加扰比特 $y_t,y_{t-1},\cdots,y_{t-p}$ 可恢复出相应的卷积码比特 c_t，实现解扰，因此自同步扰码的盲识别可归结为其反馈多项式的识别。本文针对 BPSK 调制信号，利用相关解调器输出的软判决序列实现置于卷积编码之后的自同步扰码的盲识别。

3 反馈多项式系数的代价函数的建立及求解

3.1 基于校验向量的新序列生成

对于 (n,k,m) 卷积码，存在 $(n-k)\times n$ 的校验多项式矩阵 $\boldsymbol{H}\ D$ 与编码序列 $\boldsymbol{c}\ D$ 满足正交关系[17]：

$$\boldsymbol{c}\ D\cdot\boldsymbol{H}^{\mathrm{T}}\ D=\boldsymbol{0} \tag{3}$$

若校验多项式矩阵中各项的最高阶数为 μ，那么由校验多项式的系数能够得到 $(n-k)\times n(\mu+1)$ 的基本校验矩阵 $\boldsymbol{H}_{\mathrm{b}}$。由式(3)可知，基本校验矩阵 $\boldsymbol{H}_{\mathrm{b}}$ 与长度为 $n(\mu+1)$ 的截段码字 $\boldsymbol{c}$ 满足如式(4)所示的正交关系。

$$\boldsymbol{c}\cdot\boldsymbol{H}_{\mathrm{b}}^{\mathrm{T}}=\boldsymbol{0} \tag{4}$$

基本校验矩阵的行向量为卷积码的校验向量 $\boldsymbol{h}$ [18]，由式(4)可知卷积码的截段码字与其任意校验向量均满足正交关系 $\boldsymbol{c}\cdot\boldsymbol{h}^{\mathrm{T}}=0$。根据这一正交关系，可利用自同步加扰序列及校验向量生成新的序列。将卷积码自同步加扰序列 $y_t,t>0$ 进行分块，每个加扰数据块的长度与校验向量的长度相同，相邻数据块的起始点相差一个码元，那么第 t 个数据块可表示为 $\boldsymbol{y}_t=\left[y_t\ y_{t+1}\cdots y_{t+n(\mu+1)-1}\right]$。将 $\boldsymbol{y}_t$ 与校验向量 $\boldsymbol{h}$ 相乘，得到

$$\begin{aligned}\boldsymbol{y}_t\cdot\boldsymbol{h}^{\mathrm{T}}&=\boldsymbol{c}_t\cdot\boldsymbol{h}^{\mathrm{T}}\oplus a_1\boldsymbol{y}_{t-1}\cdot\boldsymbol{h}^{\mathrm{T}}\\&\quad\oplus a_2\boldsymbol{y}_{t-2}\cdot\boldsymbol{h}^{\mathrm{T}}\oplus\cdots\oplus a_p\boldsymbol{y}_{t-p}\cdot\boldsymbol{h}^{\mathrm{T}}\end{aligned} \tag{5}$$

设 $z_t=\boldsymbol{y}_t\cdot\boldsymbol{h}^{\mathrm{T}}$，那么加扰数据块与校验向量相乘后的输出序列可表示为 $z_t,t>0$。

3.2 基于软判决的代价函数的建立

当 $t=Kn+1,K\in\mathrm{N}^+$，且 $t>p$ 时，由于 $\boldsymbol{c}_t\cdot\boldsymbol{h}^{\mathrm{T}}=0$，那么序列 $z_t,z_{t-1},\cdots,z_{t-p}$ 满足式(6)所示的线性关系。

$$z_t=a_1z_{t-1}\oplus a_2z_{t-2}\oplus\cdots\oplus a_pz_{t-p} \tag{6}$$

从概率的角度可将式(6)阐释为等式 $\overset{p}{\underset{j=0}{\oplus}}a_jz_{t-j}=1$ 成立的概率为零，即

$$P\left(\overset{p}{\underset{j=0}{\oplus}}a_jz_{t-j}=1\right)=0 \tag{7}$$

式中，$a_0=1$。下面推导式(7)的解析表达式，首先给出关于 GF(2) 域上变量概率运算的定理 1。

定理 1[19]　若 $b_i\ 1\le i\le q$ 是 GF(2) 域上相互独立的随机变量，则 $b_i\ 1\le i\le q$ 满足式(8)所示概率运算。

$$P\ \overset{q}{\underset{i=1}{\oplus}}b_i=1\ =\frac{1}{2}-\frac{1}{2}\prod_{i=1}^{q}1-2P\ b_i=1 \tag{8}$$

由于序列 $z_t,t>0$ 的各元素相互独立，各反馈多项式系数 $a_j,1\le j\le p$ 相互独立，且 $z_t,t>0$ 与 $a_j,1\le j\le p$ 间也相互独立，那么根据定理 1 得到

$$\begin{aligned}&P\left(\overset{p}{\underset{j=0}{\oplus}}a_jz_{t-j}=1\right)\\&=\frac{1}{2}-\frac{1}{2}\prod_{j=0}^{p}1-2P\ a_j=1\ P\ z_{t-j}=1\end{aligned} \tag{9}$$

由 $z_{t-j}=\boldsymbol{y}_{t-j}\cdot\boldsymbol{h}^{\mathrm{T}}$ 可知概率 $P\ z_{t-j}=1$ 为

$$P\ z_{t-j}=1\ =\frac{1}{2}-\frac{1}{2}\prod_{q=0}^{n(\mu+1)-1}1-2P\ y_{t-j+q}h_q=1 \tag{10}$$

式中，$h_q\ 0\le q\le n(\mu+1)-1$ 表示校验向量 $\boldsymbol{h}$ 的第 $q+1$ 个元素。进一步化简概率 $P\ y_{t-j+q}h_q=1$ 得到

$$P\ y_{t-j+q}h_q=1\ =\begin{cases}0, & h_q=0\\ P\ y_{t-j+q}=1\ , & h_q=1\end{cases} \tag{11}$$

将式(11)代入到式(10)中，得到

$$P\ z_{t-j}=1\ =\frac{1}{2}-\frac{1}{2}\prod_{q|h_q=1}1-2P\ y_{t-j+q}=1 \tag{12}$$

受误码影响，由解调及检测判决后得到的二进制比特信息无法获知加扰比特 y_t 为 1 的概率 $P(y_t=1)$，但利用解调输出的软判决数据 r_t 可得到其后验概率 $P\ y_t=1|r_t$。软判决数据中含有加扰比特的可靠度信息[20–22]，对于 BPSK 调制信号，软判决数据 r_t 与相对应的加扰比特 y_t 满足关系：

$$\left.\begin{aligned}r_t&=+1+n_t,\ y_t=0\\ r_t&=-1+n_t,\ y_t=1\end{aligned}\right\} \tag{13}$$

式中，n_t 为高斯白噪声。根据式(13)可得后验概率 $P\ y_t=1|r_t$ 为[20]

$$P\ y_t=1|r_t\ =\frac{\mathrm{e}^{-2r_t/\sigma^2}}{\mathrm{e}^{-2r_t/\sigma^2}+1} \tag{14}$$

式中，σ^2 为噪声方差。

假设概率 $P\ a_j=1\ =\eta_j\ 1\le j\le p$ ，结合式(9)，式(12)，式(14)得到概率 $P\left(\bigoplus_{j=0}^{p}a_jz_{t-j}=1\right)$ 的近似值为

$$P\left(\bigoplus_{j=0}^{p}a_jz_{t-j}=1\right)\approx\frac{1}{2}-\frac{1}{2}\prod_{j=0}^{p}\left\{1-\eta_j\left[1-\prod_{q|h_q=1}\left(1-2\frac{\mathrm{e}^{-2r_{t-j+q}/\sigma^2}}{\mathrm{e}^{-2r_{t-j+q}/\sigma^2}+1}\right)\right]\right\}\tag{15}$$

最小化概率 $P\left(\bigoplus_{j=0}^{p}a_jz_{t-j}=1\right)$ 的同时也就是最大化序列 $z_t,z_{t-1},\cdots,z_{t-p}$ 线性关系的成立概率。若序列 $z_t,t>0$ 中包含 N 组式(6)的线性关系，那么反馈多项式的识别可建模为式(16)所示的优化问题。

$$\min\frac{N}{2}-\frac{1}{2}\sum_{K=1}^{N}\prod_{j=0}^{p}\left(1-\eta_j\cdot\left(1-\prod_{q|h_q=1}\left(1-2\frac{\mathrm{e}^{-2r_{Kn-j+q}/\sigma^2}}{\mathrm{e}^{-2r_{Kn-j+q}/\sigma^2}+1}\right)\right)\right)\tag{16}$$

优化求解出参数 η_j 后，根据式(17)的判决规则可估计出反馈多项式系数。

$$\left.\begin{aligned}a_j&=1,\ \eta_j\ge0.5\\a_j&=0,\ \eta_j<0.5\end{aligned}\right\}\tag{17}$$

3.3 基于元素值约束的动态搜索烟花算法的代价函数求解

动态搜索烟花算法属于群体智能算法的范畴，其具有优良的全局寻优能力和广泛的适用性[23]，较基本烟花算法[24]有着更快的收敛速度和更高的求解精度。本文在利用动态搜索烟花算法求解代价函数时，结合自同步扰码的反馈多项式多为 2 项式、3 项式和 5 项式的特点[8,9]，在原动态搜索烟花算法的基础上增加烟花个体元素值约束操作，将每个烟花个体中大于 0.5 的元素值个数约束在区间[2,5]内。元素值约束的动态搜索烟花算法的流程图如图 3 所示，下面对算法流程图中的各个步骤进行说明。

(1)初始化烟花种群：种群中每个烟花个体 $\left[1\ \eta_1\ \eta_2\cdots\eta_p\right]$ 表示一个反馈多项式系数向量，其中 $\eta_j\sim U\ (0,1)\ ,\ 1\le j\le p\ ,\ p$ 为反馈多项式的阶数，若阶数未知，将 p 取一个较大值。

(2)烟花个体元素值约束操作：统计烟花个体中大于 0.5 的元素值个数 n'，对于 $n'>5$ 或 $n'<2$ 的烟花个体，将其中大于 0.5 的元素值个数约束在区间[2,5]内。

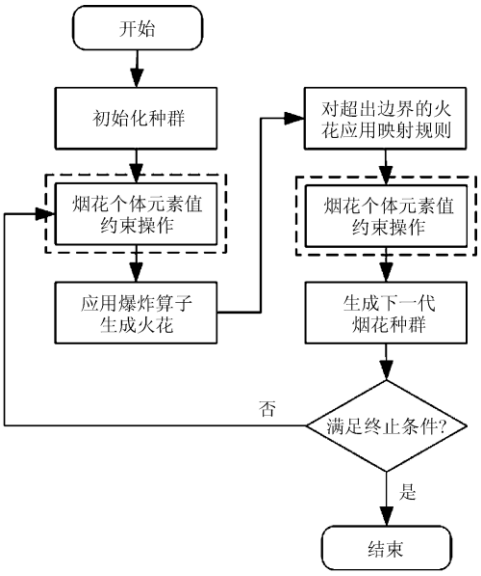

图 3 元素值约束的动态搜索烟花算法流程图

烟花个体中第 1 个元素恒为常数 1，若某个烟花个体的第 2 个至最后一个元素间有 n'' 个元素值大于 0.5，且 $n''>4$，那么随机地从这 n'' 个元素中选择 $n''-4$ 个元素，$i_q\ 1\le q\le n''-4$ 分别表示这 $n''-4$ 个元素在烟花个体中的位置，执行操作 $\eta_{i_q}=\eta_{i_q}-0.5\ 1\le q\le n''-4$ 。

若某个烟花个体的第 2 个至最后一个元素间不存在大于 0.5 的元素值，即 $n''=0$，那么随机地从第 2 个至最后一个元素间选择 1 个元素，i_1 表示该元素的位置，执行操作 $\eta_{i_1}=\eta_{i_1}+0.5$。

(3)爆炸操作：首先根据烟花个体的适应度值 $g_k\ 1\le k\le N_{\mathrm{f}}$ 计算烟花个体爆炸产生的火花数 S_k。

$$S_k=m\frac{\max\limits_{1\le k\le N_{\mathrm{f}}}g_k-g_k+\alpha}{\sum\limits_{k=1}^{N_{\mathrm{f}}}\left(\max\limits_{1\le k\le N_{\mathrm{f}}}g_k-g_k\right)+\alpha}\tag{18}$$

式中，N_{f} 是种群中烟花个体数目，m 是产生的火花总数，α 是为保证分母不为零的极小的常数。

然后计算核心烟花与非核心烟花的爆炸半径。核心烟花爆炸半径 A_{cf} 的计算式为

$$A_{\mathrm{cf}}=\begin{cases}C_{\mathrm{a}}\cdot A'_{\mathrm{cf}},\ g_{\mathrm{cf}}-g'_{\mathrm{cf}}>0\\C_{\mathrm{r}}\cdot A'_{\mathrm{cf}},\ g_{\mathrm{cf}}-g'_{\mathrm{cf}}=0\end{cases}\tag{19}$$

式中，A'_{cf} 为上次迭代的核心烟花的爆炸半径，g_{cf} 和 g'_{cf} 分别表示本次迭代和上次迭代的核心烟花的适应度值，放大因子 $C_{\mathrm{a}}>1$，缩小因子 $C_{\mathrm{r}}<1$。

非核心烟花的爆炸半径 A_k 的计算式为

$$A_k = A_{\max}\frac{g_k - g_{\mathrm{cf}} + \alpha}{\sum_{k=1}^{N_{\mathrm{f}}} g_k - g_{\mathrm{cf}} + \alpha} \tag{20}$$

式中，$A_{\max}$为非核心烟花的最大爆炸半径。

最后通过对烟花个体的元素值进行位移来产生火花，如式(21)所示。

$$\eta'_{k,j} = \begin{cases} \eta_{k,j} + U\ 0, A_k\ , & x_{k,j} \geq 0.5 \\ \eta_{k,j}, & x_{k,j} < 0.5 \end{cases}, \quad 1 \leq j \leq p \tag{21}$$

式中，$x_{k,j} \sim U\ 0,1\ $。

(4)映射操作：将火花中超出可行域的元素值映射到区间 $0,1\ $ 内。

(5)生成下一代烟花种群：首先对产生的火花执行步骤(2)；然后执行精英—随机选择策略，保留烟花及火花中适应度值最大的个体，并从剩余的烟花及火花中随机选择出 $N_{\mathrm{f}}-1$ 个个体构成下一代烟花种群。

(6)判定是否满足算法终止条件：若不满足算法终止条件，则重复步骤(3)~步骤(5)，直到达到最大迭代次数或代价函数值小于设定的门限值为止。

3.4 算法计算复杂度分析

本文方法的计算量由两部分构成，一部分是加扰数据块与校验向量相乘来生成新序列，另一部分是利用改进的动态搜索烟花算法优化求解代价函数。若校验向量的长度为L，新生成序列的长度为N'，那么生成新序列所需的计算量为$N'(2L-1)$。利用改进的动态搜索烟花算法求解代价函数的计算量集中在计算烟花个体及产生的火花的适应度值。若烟花个体的维数为d，新生成的序列 $z_t, t>0$ 中包含N组线性约束关系，那么计算每个烟花个体适应度值所需的计算量为$3Nd$。设每个烟花种群中包含N_{f}个烟花个体，爆炸操作产生的火花总数为m，那么每次迭代运算中计算烟花个体及火花的适应度值所需的计算量为$3\ N_{\mathrm{f}}+m\ Nd$。若迭代次数为T，那么本文方法的计算复杂度为$O\ 3\ N_{\mathrm{f}}+m\ TNd+2N'L\ $。

4　仿真分析

实验 1　验证本文方法的有效性。实验中自同步扰码的反馈多项式为$f(x)=1+x^2+x^5$，卷积码为$(2,1,4)$卷积码，其生成多项式矩阵为$\left[1+x^3+x^4,\ 1+x+x^2+x^4\right]$。信噪比为10 dB，数据量为150 bit。烟花种群的个体数量为5，个体的维数设为9。核心烟花初始爆炸半径为 1，其爆炸半径的放大因子$C_{\mathrm{a}}=1.2$，缩小因子$C_{\mathrm{r}}=0.8$，非核心烟花的最大爆炸半径为0.8，每次迭代产生的火花数为150，迭代次数为200次。分别利用原动态搜索烟花算法和本文的改进算法优化求解代价函数，代价函数值随迭代次数变化曲线如图4所示。

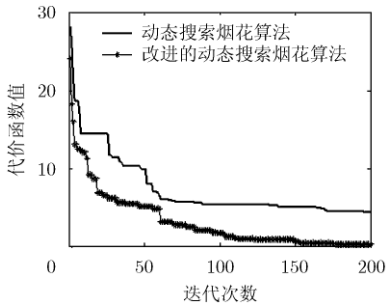

图 4 代价函数值随迭代次数变化曲线

由图4可知，随着迭代次数的增加，代价函数值逐渐减小，且利用本文的改进算法优化求解代价函数时，代价函数值下降速度更快，说明相比于原动态搜索烟花算法，改进算法有着更快的收敛速度。当迭代到200次时，代价函数值为0.2093，此时核心烟花为$\left[1,9\times10^{-4},0.9986,0,3\times10^{-4},1,5\times10^{-4},\ 5\times10^{-4},0\right]$，进一步根据式(17)所示的判决规则，识别自同步扰码的反馈多项式为$\hat{f}(x)=1+x^2+x^5$。由$\hat{f}(x)=f(x)$可知，本文方法能够在自同步扰码阶数未知的情况下有效地实现反馈多项式的识别。

为了进一步说明本文方法的有效性，实验中采用不同的卷积码和自同步扰码，所采用的$(2,1,7)$, $(3,1,4)$ 和 $(3,2,2)$ 卷积码的生成多项式矩阵分别为$\left[1+x^2+x^5+x^6+x^7,\ 1+x+x^2+x^3+x^4+x^7\right]$, $\left[1+x^2+x^4,1+x+x^3+x^4,1+x+x^2+x^3+x^4\right]$ 和 $\begin{bmatrix}1+x^2 & 1 & x\\ x & 1+x^2 & 1+x+x^2\end{bmatrix}$，其他实验条件不变。在不同的卷积码和自同步扰码条件下，本文方法的识别结果如表1所示。

表 1 不同卷积码及自同步扰码条件下的识别结果

卷积码码型	自同步扰码	求解所得的核心烟花	识别结果
$(2,1,7)$	$1+x^5+x^6$	$\left[1,5\times10^{-4},8\times10^{-4},2\times10^{-4},0,0.9996,0,9992,3\times10^{-4},8\times10^{-4}\right]$	$1+x^5+x^6$
$(3,1,4)$	$1+x^3+x^7$	$\left[1,0,4\times10^{-4},0.9995,0,8\times10^{-4},3\times10^{-4},0.9998,6\times10^{-4}\right]$	$1+x^3+x^7$
$(3,2,3)$	$1+x+x^5+x^6+x^8$	$\left[1,0.9980,2\times10^{-4},2\times10^{-4},0.0011,0.9984,0.9974,0,0.9996\right]$	$1+x+x^5+x^6+x^8$

由表 1 可知，当实验中采用不同的卷积码和自同步扰码时，本文方法均能够正确识别出自同步扰码的反馈多项式。

实验 2 比较在不同信噪比条件下，利用改进的动态搜索烟花算法、基本烟花算法以及穷举搜索算法求解构造的代价函数时的识别正确率。实验中自同步扰码的反馈多项式为$1+x^3+x^7$，(2,1,4)卷积码生成多项式矩阵为$\left[1,1+x^2+x^4\right]$，数据量为 400 bit。烟花个体维数设为 8，烟花算法的迭代次数设为 100 次。信噪比的变化范围是 0~10 dB，相邻信噪比相差 1 dB，其他条件同实验 1。不同信噪比下 3 种求解算法的识别正确率如图 5 所示。

由图 5 可知，利用改进的动态搜索烟花算法求解代价函数时的识别正确率与利用穷举搜索算法求解时的识别正确率接近，且大于基本烟花算法的识别正确率，从而说明改进的动态搜索烟花算法具有优良的全局收敛性能。此外，实验结果表明本文方法在高斯白噪声背景下具有较好的鲁棒性。

实验 3 分析本文方法的识别正确率与数据量的关系。实验中自同步扰码的反馈多项式为$1+x^3+x^{10}$，数据量分别为 200 bit, 400 bit, 600 bit 和 800 bit，烟花个体的维数设为 16，其他实验条件同实验 2。不同数据量下，本文方法识别的正确率随信噪比变化曲线如图 6 所示。

由图 6 可知，相同信噪比条件下，随着数据量的增大，本文方法的识别正确率逐渐提高。实验结果表明在中等信噪比条件下，数据量达到10^3数量级时本文方法就能取得很好的识别效果，所需数据量较小。

实验 4 分析识别的正确率与反馈多项式阶数的关系。实验中反馈多项式分别为$1+x^3+x^7$，$1+x^2+x^{11}$和$1+x+x^{15}$，数据量为 600 bit，针对不同阶数的反馈多项式，烟花个体的维数分别设为 8, 12 和 16。信噪比的变化范围是 0~10 dB，其他条件同实验 2。本文方法对不同阶数的反馈多项式识别正确率如图 7 所示。

由图 7 可知，相同信噪比及数据量的条件下，随着反馈多项式阶数的减小，识别的正确率逐渐提高。

5 结论

本文提出了一种基于代价函数求解的卷积码自同步加扰的扰码盲识别方法。该方法首先将自同步加扰数据块与卷积码校验向量相乘来产生新的序列；然后利用软判决序列建立了以反馈多项式系数为参量的代价函数；最后基于改进的动态搜索烟花算法优化求解代价函数，由求解得到的参量值识别出反馈多项式。该方法能够在自同步扰码阶数未知的情况下有效地识别出反馈多项式，无需对反馈多项式遍历搜索，且具有较好的鲁棒性，所需数据量小，随着数据量的增大和扰码阶数的降低，其识别正确率逐渐提高。此外，本文方法可拓展应用于线性分组码自同步加扰的扰码盲识别。

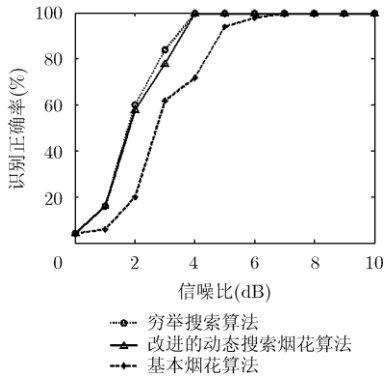

图 5 识别正确率随信噪比变化曲线

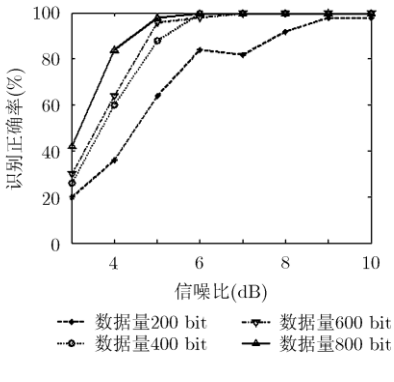

图 6 识别正确率与数据量关系

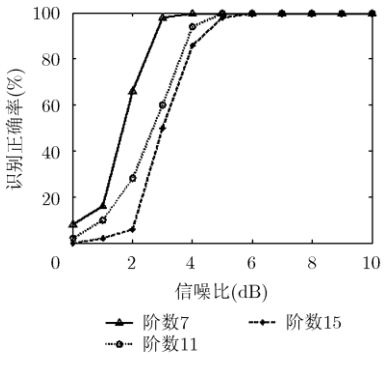

图 7 识别正确率与扰码阶数的关系

参 考 文 献

[1] 李相迎. CCSDS数据链路层协议识别关键技术研究[D]. [博士论文], 中国科学院空间科学与应用研究中心, 2011: 21-23.
LI Xiangying. Key technologies of protocol identification for CCSDS data link layer[D]. [Ph.D. dissertation], Center for Space Science and Applied Research Chinese Academy of Sciences, 2011: 21-23.

[2] SUN Yongwei, ZHANG Limin, and MA Yu. Reconstruction of linear scrambler with block data[J]. *Applied Mechanics and Materials*, 2015, 701(5): 114-118. doi: 10.4028/AMM.701-702.114.

[3] 张永光, 楼才义. 信道编码及其识别分析[M]. 北京: 电子工业出版社, 2010: 6-7.
ZHANG Yongguang and LOU Caiyi. Channel Encoder and Identification Analysis[M]. Beijing: Publishing House of Electronics Industry, 2010: 6-7.

[4] 马钰, 张立民. 基于实时检测的扰码重建算法[J]. 电子与信息

学报, 2016, 38(7): 1794–1799. doi: 10.11999/JEIT151068.
MA Yu and ZANG Limin. Reconstruction of scrambler with real-time test[J]. *Journal of Electronics & Information Technology*, 2016, 38(7): 1794–1799. doi: 10.11999/JEIT 151068.

[5] 杨忠立, 刘玉君. 自同步扰乱序列的综合算法研究[J]. 信息技术, 2005, 5(2): 30–32. doi: 10.13274/j.cnki.hdzj.2005.02.011.
YANG Zhongli and LIU Yujun. Algorithm research of self-synchronizing scrambler sequence[J]. *Information Technology*, 2005, 5(2): 30–32. doi: 10.13274/j.cnki.hdzj.2005. 02.011.

[6] 吕喜在, 苏绍璟, 黄芝平. 一种新的自同步扰码多项式盲恢复方法[J]. 兵工学报, 2011, 32(6): 680–685.
LÜ Xizai, SU Shaojing, and HUANG Zhiping. A novel blind recovery method of self-synchronizing scrambling polynomial [J]. *Acta Armentarii*, 2011, 32(6): 680–685.

[7] 黄芝平, 周靖, 苏绍璟, 等. 基于游程统计的自同步扰码多项式阶数估计[J]. 电子科技大学学报, 2013, 42(4): 541–545. doi: 10.3969/j.issn.1001-0548.2013.04.002.
HUANG Zhiping, ZHOU Jing, SU Shaojing, *et al*. Order estimation of self-synchronizing scrambling polynomial based on run statistic[J]. *Journal of University of Electronic Science and Technology of China*, 2013, 42(4): 541–545. doi: 10.3969 /j.issn.1001-0548.2013.04.002.

[8] 廖红舒, 袁叶, 甘露. 自同步扰码的盲识别方法[J]. 通信学报, 2013, 34(1): 136–143. doi: 10.3969/j.issn.1000-436x.2013.01. 016.
LIAO Hongshu, YUAN Ye, and GAN Lu. Novel blind recognition method for self-synchronized scrambler[J]. *Journal on Communications*, 2013, 34(1): 136–143. doi: 10.3969/j.issn.1000-436x.2013.01.016.

[9] CLUZEAU M. Reconstruction of a linear scrambler[J]. *IEEE Transactions on Computers*, 2007, 56(9): 1283–1291.

[10] 陈泽亮, 彭华, 巩克现, 等. 基于软信息的扰码盲识别方法[J]. 通信学报, 2017, 38(3): 174–182. doi: 10.11959/j.issn.1000-436x.2017043.
CHEN Zeliang, PENG Hua, GONG Kexian, *et al*. Scrambler blind recognition method based on soft information[J]. *Journal on Communications*, 2017, 38(3): 174–182. doi: 10.11959/j.issn.1000-436x.2017043.

[11] 马钰, 张立民, 王好同. 编码加扰序列的帧同步盲识别[J]. 电子学报, 2016, 44(9): 2087–2092. doi: 10.3969/j.issn.0372-2112. 2016.09.010.
MA Yu, ZHANG Limin, and WANG Haotong. Blind identification of frame synchronization in scrambled code sequence[J]. *Acta Electronic Sinica*, 2016, 44(9): 2087–2092. doi: 10.3969/j.issn.0372-2112.2016.09.010.

[12] LIU Xiaobei, KOH S N, CHUI C C, *et al*. A study on reconstruction of linear scrambler using dual words of channel encoder[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(3): 542–552. doi: 10.1109/ TIFS.2013.2246515.

[13] MA Yu, ZHANG Limin, and WANG Haotong. Reconstructing synchronous scrambler with robust detection capability in the presence of noise[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(2): 397–408. doi: 10.1109/TIFS.2014.2378143.

[14] LI Xinhao, ZHANG Min, HAN Shunan, *et al*. Distinction of self-synchronous scrambled linear block codes based on multi-fractal spectrum[J]. *Journal of Systems Engineering and Electronics*, 2016, 27(5): 968–978. doi: 10.21629/JSEE. 2016.05.04.

[15] 张旻, 吕全通, 朱宇轩. 基于线性分组码的自同步扰码盲识别[J]. 应用科学学报, 2015, 33(2): 178–186. doi: 10.3969/j.issn. 0255-8297.2015.02.007.
ZHANG Min, LÜ Quantong, and ZHU Yuxuan. Blind recognition of self-synchronized scrambler based on linear block code[J]. *Journal of Applied Sciences*, 2015, 33(2): 178–186. doi: 10.3969/j.issn.0255-8297.2015.02.007.

[16] 吕全通, 张旻, 李歆昊, 等. 基于码重分布距离的自同步扰码识别方法[J]. 探测与控制学报, 2015, 37(5): 7–13.
LÜ Quantong, ZHANG Min, LI Xinhao, *et al*. Self-synchronized scrambler recognition based on code weight distributing distance[J]. *Journal of Detection & Control*, 2015, 37(5): 7–13.

[17] HUANG Li, CHEN Wengu, CHEN Enhong, *et al*. Blind recognition of k/n rate convolutional encoders from noisy observation[J]. *Journal of Systems Engineering and Electronics*, 2017, 28(2): 235–243. doi: 10.21629/JSEE.2017. 02.04.

[18] SOTEH A G and BIZAKI H K. On the analytical solution of rank problem in the convolutional code identification context [J]. *IEEE Communications Letters*, 2016, 20(3): 442–445. doi: 10.1109/LCOMM.2016.2519519.

[19] HAGENAUER J, OFFER E, and PAPKE J. Iterative decoding of binary block and convolutional codes[J]. *IEEE Transctions on Information Theory*, 1996, 42(2): 429–445.

[20] YU Peidong, LI Jing, and PENG Hua. A least square method for parameter estimation of RSC sub-codes of turbo codes[J]. *IEEE Communications Letters*, 2014, 18(4): 644–647. doi: 10.1109/LCOMM.2014.022514.140086.

[21] 刘骏, 李静, 于沛东. 一种Turbo码随机交织器的迭代估计方法[J]. 通信学报. 2015, 36(6): 1401–1406. doi: 10.11959/j.issn. 1000-436x.2015140.
LIU Jun, LI Jing, and YU Peidong. Iterative estimation method for random interleaver of Turbo codes[J]. *Journal on Communications*, 2015, 36(6): 1401–1406. doi: 10.11959/ j.issn.1000-436x.2015140.

[22] 刘杰, 张立民, 钟兆根, 等. 一种软判决下的本原BCH码盲识别方法[J]. 西安交通大学学报, 2017, 51(6): 59–65. doi: 10.7652/xjtuxb201706010.
LIU Jie, ZHANG Limin, ZHONG Zhaogen, *et al*. A blind recognition method for primitive BCH codes in soft decision situations[J]. *Journal of Xi' an Jiaotong University*, 2017, 51(6): 59–65. doi: 10.7652/xjtuxb201706010.

[23] ZHENG Shaoqiu, JANECEK A, LI Junzhi, *et al*. Dynamic search in fireworks algorithm[C]. IEEE Congress on Evolutionary Computation, Beijing, China, 2014: 3222–3229. doi:10.1109/CEC.2014.6900485.

[24] TAN Ying and ZHU Yuanchun. Fireworks algorithm for optimization[C]. International Conference in Swarm Intelligence, Berlin, Germany, 2010: 355–364. doi: 10.1007/ 978-3-642-13495-1-44.

韩树楠：　男，1989 年生，博士生，研究方向为信道编码识别.
张　旻：　男，1966 年生，教授，博士，研究方向为通信信号处理、智能计算.
李歆昊：　男，1989 年生，讲师，博士，研究方向为信道编码识别与协议分析.