编码加扰序列的帧同步盲识别

马 钰,张立民,王好同
(海军航空工程学院电子信息工程系,山东烟台 264001)

摘 要: 在同步情况下,基于对偶码可有效重建线性扰码的反馈关系,但非合作通信方同样需要完成盲同步.在无噪声条件下,针对编码加扰序列的盲同步问题,结合反馈多项式检测提出了帧同步盲识别算法.利用初始帧同步中探测的反馈多项式倍式集,可同时完成扰码反馈多项式和扰码序列的估计.实现初始同步后,可借助解扰数据帧结构属性完成精确同步;然后,将算法推广到了含噪信道情况;最后,基于 Walsh-Hadamard 变换给出了检测统计量的规范计算方案,以降低计算复杂度.

关键词: 对偶码; 帧同步扰码; 线性反馈移位寄存器; 盲同步; Walsh-Hadamard 变换
中图分类号: TN919 **文献标识码:** A **文章编号:** 0372-2112 (2016)09-2087-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.09.010

Blind Identification of Frame Synchronization in Scrambled Coding Sequence

MA Yu, ZHANG Li-min, WANG Hao-tong
(*Department of Electronic and Information Engineering, Naval Aeronautical and Astronautical University, Yantai, Shandong* 264001, *China*)

Abstract: With a dual word, we can reconstruct the feedback polynomial of a linear scrambler when the synchronization is complete. An eavesdropper must achieve synchronization before recovering scrambler. Based on the algorithm of reconstruction of linear scrambler, we present techniques to achieve blind synchronization. We can get a set of multiples of the feedback polynomial when course synchronization is complete. Meantime, we can also recover the feedback polynomial and a scrambler sequence. Then, we need architecture of frame to achieve fine synchronization with the descrambled data. The study is based on the assumption that the channel is noiseless and then extended to the noisy channel condition. In order to reduce the computational complexity, we also propose a normal scheme to compute the statistic on the base of Walsh-Hadamard transformation.

Key words: dual word; frame synchronous scrambler; linear feedback shift register (LFSR); blind synchronization; Walsh-Hadamard transformation

1 引言

在数字通信中,通过序列加扰的方式可以将信息序列变换成近似随机的序列.在通信参数缺失的情况下,非合作第三方需要排除干扰并恢复扰码序列,才能获得信息序列.通信中数据往往按帧传输,因此在恢复扰码之前,需要首先完成帧同步.

线性扰码分为同步扰码和自同步扰码两种类型,可通过线性反馈移位寄存器(LFSR)产生.因为自同步扰码具有误码扩散特性,所以在无线通信中通常使用同步扰码.由于信道编码后信源的有偏性几乎消失[1],再加上扰码序列本身具有伪随机特性,所以在扰码未知的情况下基于相关分析的盲同步方案[2]将不再直接适用.因此,考虑结合扰码重建算法进行帧同步盲识别.

非合作直接序列扩频信号中的伪随机(PN)序列估计算法[3~5],由于其中 PN 序列的线性复杂度相对较低,以及和信息的作用方式,与扰码序列存在显著差别,所以不适用于扰码重建.扰码重建主要包括两个方面:反馈多项式的检测和初始状态的恢复[6].文献[7]利用组合枚举和快速相关攻击构建了伪随机扰码的快速盲恢复,其中利用组合枚举求解反馈函数的方法,在抽头系数较少的情况下才较为适用;文献[8]提出了基于 Walsh-Hadamard 变换的含错扰码序列生成多项式测定算法,其需要较为准确的估计反馈函数的阶数信息;文

收稿日期:2015-01-21;修回日期:2016-01-06;责任编辑:蓝红杰
基金项目:泰山学者工程专项经费

献[9]给出了含错 m 序列本原多项式的高阶统计测定算法,核心算法本质上与文献[6]中检测信源有偏性一致,不同在于模型中将误码视为一种有偏性较大的信源. 但上述算法模型中均未考虑原始信息序列,仅是对扰码序列本身或受到信道误码后的攻击. 基于信源有偏性 Cluzeau 提出了搜索低重量倍式的反馈多项式检测算法[6];为提高检测性能,文献[10]进一步修正了假设中的方差参数,提出了避免错误检测的方案;假设源 bit 流经前向纠错编码之后被加扰,文献[1]使用对偶码进行了扰码序列重建;文献[11]进一步提高了文献[1]中重建算法在含噪信道中的性能. 通信中数据往往按照一定分组或帧进行传输,本文将结合基于对偶码的扰码重建技术,研究帧同步的盲识别问题.

2 系统模型

同步扰码器将输入信息序列与伪随机序列组合生成加扰序列,因为 LFSR 具有良好的统计特性和便于硬件实现,所以通常使用 LFSR 产生伪随机的扰码序列. 一个 LFSR 序列可通过反馈多项式和初始状态唯一确定. 将信息序列经编码后与扰码序列$\{s_t\}$进行模-2 加,生成加扰序列$\{y_t\}$(图 1,图 2),即 $y_t = c_t \oplus s_t, t \geqslant 0$ 其中⊕表示模-2 加运算.

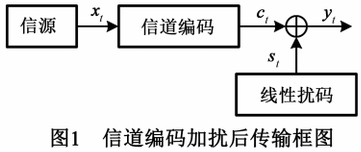

图1 信道编码加扰后传输框图

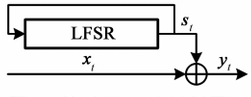

图2 线性同步扰码框图

考虑线性分组码作为信道编码的情况,对于(n,k)线性分组码 C,其中 k 是信息 bit 数量,n 是编码 bit 数量,生成矩阵可表示为 $k \times n$ 维矩阵 $\boldsymbol{G}$. 编码器可将 k 个 bit 的信息 $\boldsymbol{x} = [x_0, x_1, \cdots, x_{k-1}]$ 变换成 n 个 bit 的码字 $\boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}]$. 假设 C 的校验矩阵为$(n-k) \times n$ 维矩阵 $\boldsymbol{H}$,$\boldsymbol{H}$ 的行向量 $\boldsymbol{h}_0, \boldsymbol{h}_1, \cdots, \boldsymbol{h}_{n-k-1}$ 可扩展为对偶空间 $C^{\perp}$. C 中任意码字正交于所有 $\boldsymbol{H}$ 的行向量,即对任意 $\boldsymbol{c} \in C$,$\boldsymbol{c}\boldsymbol{H}^{\mathrm{T}} = \boldsymbol{0}$. $\boldsymbol{h}_0, \boldsymbol{h}_1, \cdots, \boldsymbol{h}_{n-k-1}$ 称为对偶码.

令 L 表示 LFSR 的长度,$P(x)$ 表示 LFSR 的反馈多项式. 如果 $P(x) = 1 + c_1 x + \cdots + c_L x^L$,那么,由 LFSR 生成序列满足 $s_{t+L} = c_1 s_{t+L-1} \oplus c_2 s_{t+L-2} \oplus \cdots \oplus c_L s_t, t \geqslant 0$. 其中 $c_1, \cdots, c_L \in \{0,1\}$.

编码后序列以 N_b 个 bit 组成一帧(图 3),其中 N_b 可被 n 整除(令 $N_f = N_b/n$),每帧信息使用相同的扰码进行加扰. 帧同步过程建模为,确定接收 bit 位置到帧起始 bit 位置的偏移量 Δt(图 4),$-N_b + 1 \leqslant \Delta t \leqslant N_b - 1$.

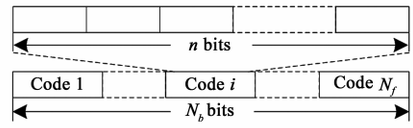

图3 帧结构

图4 帧同步模型

3 无噪声情况下帧同步算法

利用信号相关性是盲同步算法常采用的方案,例如基于自相关矩阵的 Frobenius 范数[2],或者基于数据的似然性[13]等. 下面以相关函数为例分析加扰数据的相关性,由扰码序列的伪随机特性得,

$$\mathrm{E}\{y_i \oplus y_{j+N_b}\} = \mathrm{E}\{s_i \oplus c \oplus s_j \oplus c'\} = \begin{cases} \mathrm{E}\{c \oplus c'\}, & i = j \\ 1/2, & i \neq j \end{cases} \tag{1}$$

其中 c 和 c' 表示数据 bit. 当数据 bit 未知时,认为服从等概率分布,则 $\mathrm{E}\{c \oplus c'\}$ 也等于 1/2. 由式(1)可知,加扰后扰码的伪随机性与数据 bit 的随机性相互作用,因此,在数据未知或者扰码未知的情况下,不能利用数据间的相关性进行同步位置的盲识别,而需要联合扰码重建算法进行.

基于对偶码的扰码重建[1],首先需要将接收序列$\{y_t\}$按长度 n 进行分组得到 $\boldsymbol{y}_0, \boldsymbol{y}_1, \cdots$,即 $\boldsymbol{y}_t = [y_{nt}, \cdots, y_{(n+1)t-1}]$. 通过与对偶码进行点积运算,可生成一个新的序列$\{r_t\}$. 不失一般性,假设一对偶码为 $\boldsymbol{h}_0 = [h_{0,0}, \cdots, h_{0,n-1}]$,那么

$$r_t = \boldsymbol{y}_t \boldsymbol{h}_0^{\mathrm{T}} = \sum_{i=0}^{n-1} y_{nt+i} h_{0,i} \tag{2}$$

同步状态下,根据对偶码的性质可得,$\boldsymbol{c}_t \boldsymbol{h}_0^{\mathrm{T}} = 0$,因此 $r_t = \boldsymbol{y}_t \boldsymbol{h}_0^{\mathrm{T}} = \boldsymbol{s}_t \boldsymbol{h}_0^{\mathrm{T}}$. 根据文献[1]中命题 1 可知,对于 $Q(x) = 1 + x^{ni_1} + \cdots + x^{ni_{d-1}}, 0 < i_1 < \cdots < i_{d-1}$,当 $Q(x)$ 是 $P(x)$ 的倍式时,$r_t \oplus r_{t-i_1} \oplus \cdots \oplus r_{t-i_{d-1}} \equiv 0, i_{d-1} \leqslant t \leqslant N_b$. 根据这个性质,得到帧同步算法如算法 1.

算法 1 无噪情况下帧同步算法

(1)遍历所有可能偏移量 $\Delta t = -N_b + 1, \cdots, 0, \cdots, N_b - 1$;

(2)取出长度为 N_b 的接收 bit 序列$\{y_{\Delta t}, y_{\Delta t+1}, \cdots, y_{\Delta t+N_b-1}\}$,按长度 n 进行分组得到 $\boldsymbol{y}_{0,\Delta t}, \boldsymbol{y}_{1,\Delta t}, \cdots, \boldsymbol{y}_{N_f-1,\Delta t}$,其中 $\boldsymbol{y}_{t,\Delta t} = [y_{\Delta t+nt}, y_{\Delta t+nt+1}, \cdots, y_{\Delta t+n(t+1)-1}]$;

(3)与对偶码 $\boldsymbol{h}_0$ 进行点积运算,生成新的 bit 序列$\{r_{t,\Delta t}\}$,其中 $r_{t,\Delta t} =$

$\boldsymbol{y}_{t,\Delta t}\boldsymbol{h}_0^{\mathrm{T}}$;

(4)遍历所有候选倍式集$\{Q(x)\}$,$0<i_1<\cdots<i_{d-1}\leqslant D$;

(5)初始化 $Z=0$;

(6)t 从 i_{d-1} 增加到 N_b,计算

$$z_t=r_{t,\Delta t}\sum_{j=1}^{d-1}r_{t-i_j,\Delta t} \tag{3}$$

$Z=Z+(-1)^{z_t}$;

(7)令 $N_c=N_f-i_{d-1}+1$,如果 $Z\geqslant N_c/2$,则计算其余偏移量下的统计量 Z. 如果某一时刻使得统计量等于 N_c,那么其对应的偏移位置即为帧同步位置;

(8)重复步骤 1 至步骤 7,直到找到帧同步位置或者完成所有遍历.

上述算法中,在同步时刻检测倍式的统计量应等于 N_c,而在非同步时刻倍式检测统计量应小于 N_c,利用这一属性可实现帧同步位置的初步判别. 根据文献[1],当 $N_c=50$ 时,倍式判决的虚警概率 $P_f<10^{-10}$. 仿真验证中,初始位置偏差为 -351,搜索范围 $D=50$,$d=3,4,5$,不同情况下的仿真结果见表 1. 仿真结果中,出现连续相邻的多个同步估计位置,一方面是由于前后相邻的几个 bit 恰好满足校验关系,或者对偶空间中存在满足循环移位关系的对偶码;另一方面,编码类型对于同步算法的影响主要体现在分组长度不同上,会使得新生成序列具有不同的反馈关系[11];另外,帧长度的影响主要是体现在截取扰码序列的长度上,与初始状态的影响相似,具有随机性. 因此,此时称为粗同步,仍需要进一步处理才能确定正确的帧起始位置.

表 1　无噪情况下帧同步仿真结果

码型	帧长 N_b	反馈多项式	初始状态	估计值偏差
Hamming (7,4)	700	$1+x^2+x^3+x^4+x^8$	$[1,\boldsymbol{0}_6,1]$	0
		$1+x^3+x^4+x^6+x^9$	$[1,\boldsymbol{0}_2,1,\boldsymbol{0}_2,1,0,1]$	-7,0,7
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\boldsymbol{0}_2,1,\boldsymbol{0}_3,1]$	-7,0,7
BCH (7,4)	700	$1+x^2+x^3+x^4+x^8$	$[1,\boldsymbol{0}_6,1]$	-5,0,1,2,9
		$1+x^3+x^4+x^6+x^9$	$[1,\boldsymbol{0}_2,1,\boldsymbol{0}_2,1,0,1]$	-7,-6,0,1,2,7
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\boldsymbol{0}_2,1,\boldsymbol{0}_3,1]$	-20,-19,-14,-13,-12,-7,-6,-5,0,1,2,7,8
Hamming (7,4)	1400	$1+x^2+x^3+x^4+x^8$	$[1,\boldsymbol{0}_6,1]$	-7,0,7
		$1+x^3+x^4+x^6+x^9$	$[1,\boldsymbol{0}_2,1,\boldsymbol{0}_2,1,0,1]$	-14,-7,0
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\boldsymbol{0}_2,1,\boldsymbol{0}_3,1]$	0
BCH (7,4)	1400	$1+x^2+x^3+x^4+x^8$	$[1,\boldsymbol{0}_6,1]$	-6,0,1,2,7,9
		$1+x^3+x^4+x^6+x^9$	$[1,\boldsymbol{0}_2,1,\boldsymbol{0}_2,1,0,1]$	-26,-19,-13,-12,-7,-6,-5,0,1,2,9,16
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\boldsymbol{0}_2,1,\boldsymbol{0}_3,1]$	-56,-49,-42,-35,-28,-21,-14,-7,-6,0,1,2,7

注:$\boldsymbol{0}_n$ 表示 $1\times n$ 的全 0 向量[0 0 … 0].

在获得粗同步后,就可根据扰码重建算法恢复反馈多项式[1],并基于快速相关攻击算法[12]以及新序列与原始序列之间的关系,恢复 LFSR 的初始状态. 解扰后的数据应具有相似的帧结构特征,否则,应当在粗同步位置及其附近继续进行搜索. 当解扰后的数据出现有意义的帧结构信息时,可获得精确同步.

4　含噪情况下帧同步算法

在考虑噪声的情况下,采用二进制对称信道模型,接收 bit 序列可表示为 $y_t'=y_t(e_t$,其中 $e_t\in\{0,1\}$ 表示时刻 t 时的信道噪声,$\Pr\{e_t=0\}=0.5+\varepsilon$,$0<\varepsilon<0.5$.

$Q(x)=1+x^{i_1}+\cdots+x^{i_{d-1}}$ 是 Galois 域 GF(2)上的多项式,其重量为 d,即 $Q(x)$ 中的非零系数的数量. 令 $z_t=r_t'\oplus\sum_{j=1}^{d-1}r_{t-i_j}'$ 其中 $r_t'=\boldsymbol{y}_t'\boldsymbol{h}_0^{\mathrm{T}}$,$\boldsymbol{y}_t'=[y_{nt}',\cdots,y_{(n+1)t-1}']$. 同步状态下,$\Pr\{z_t=1\}=0.5[1-(2\varepsilon)^{wd}]$. 假设

$$\mu_1=(N_f-i_{d-1}+1)(2\varepsilon)^{wd} \tag{4}$$

$$\sigma_1^2\leqslant(N_f-i_{d-1}+1)[1+d((2\varepsilon)^{2w}-(2\varepsilon)^{2wd})] \tag{5}$$

根据文献[1]中第Ⅴ节的分析可知,如果 $Q(x)$ 是扰码序列的反馈多项式的倍式,当 $N_f\to\infty$ 时,变量 $\boldsymbol{Z}=\dfrac{\sum_{t=i_{d-1}}^{N_f}(-1)^{z_t}-\mu_1}{\sigma_1}$ 渐进服从标准正态分布. 当 $Q(x)$ 不是反馈多项式的倍式时 $\Pr\{z_t=1\}=0.5$,Z 渐进服从方差为 $N_f-i_{d-1}+1$ 的正态分布,其均值随 $Q(x)$ 变化[11].

在进行倍式判别时,可基于以下两个假设:

H_0:$Z\sim N(3\sqrt{N_f-i_{d-1}+1},N_f-i_{d-1}+1)$,$Q(x)$ 不是 $P(x)$ 的倍式;

H_1:$Z\sim N(\mu_1,\sigma_1^2)$,$Q(x)$ 是 $P(x)$ 的倍式.

非反馈多项式情况下,假设均值为 $3\sqrt{N_f-i_{d-1}+1}$ 将保证 99.7% 的测试均值落在此范围内[11]. 根据最小错误概率准则,可得到判决门限 T 应满足等式:

$$\frac{1}{\sqrt{N_c}}\exp\left\{-\frac{(T-3\sqrt{N_c})^2}{2N_c}\right\}=\frac{1}{\sigma_1}\exp\left\{-\frac{(T-\mu_1)^2}{2\sigma_1^2}\right\}$$

其中 $N_c = N_f - i_{d-1} + 1$. 将式(4)和式(5)带入上式可得:

$$T = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ 其中 } a = d[(2\varepsilon)^{2w} - (2\varepsilon)^{2wd}],$$

$$b = -[6\sqrt{N_c}(1+a) - 2N_c(2\varepsilon)^{wd}],$$

$$c = (9N_c - 2N_c\ln\sqrt{1+a})(1+a) - N_c^2(2\varepsilon)^{2wd}.$$

因此,判决的虚警概率:

$$P_f = \Pr\{Z \geqslant T \mid \mathrm{H}_0\} = 1 - \Pr\{Z < T \mid \mathrm{H}_0\} = 1 - \Phi\left(\frac{T - 3\sqrt{N_c}}{\sqrt{N_c}}\right)$$

漏报概率:

$$P_n = \Pr\{Z < T \mid \mathrm{H}_1\} = \Phi\left(\frac{T - \mu_1}{\sigma_1}\right).$$

与无噪情况下类似,得到帧同步算法如算法 2.

算法 2 含噪情况下帧同步算法

(1)遍历所有可能偏移量 $\Delta t = -N_b + 1, \cdots, 0, \cdots, N_b - 1$;

(2)取出长度为 N_b 的接收 *bit* 序列 $\{y'_{\Delta t}, y'_{\Delta t+1}, \cdots, y'_{\Delta t+N_b-1}\}$,按长度 n 进行分组得到 $y'_{0,\Delta t}, y'_{1,\Delta t}, \cdots, y'_{N_f-1,\Delta t}$,其中 $y'_{t,\Delta t} = [y'_{\Delta t+nt}, y'_{\Delta t+nt+1}, \cdots, y'_{\Delta t+n(t+1)-1}]$;

(3)与对偶码 h_0 进行点积运算,生成新的 *bit* 序列 $\{r'_{t,\Delta t}\}$,其中 $r'_{t,\Delta t} = y'_{t,\Delta t}h_0^{\mathrm{T}}$;

(4)遍历所有候选倍式集 $\{Q(x)\}$,$0 < i_1 < \cdots < i_{d-1} \leqslant D$;

(5)初始化 $Z = 0$;

(6)t 从 i_{d-1} 增加到 N_b,计算

$$z_t = r'_{t,\Delta t} \oplus \sum_{j=1}^{d-1} r'_{t-i_j,\Delta t} \tag{6}$$

$Z = Z + (-1)^{z_t}$;

(7)计算判决门限 T,均值 μ_1,标准差 σ_1. 如果 $Z \geqslant T/2$,则计算其余偏移量下的统计量 $Z(Q(x),\Delta t)$. 如果 $Z(Q(x),\Delta t) > T$,则 $Q(x)$ 为倍式,执行下一步;否则,重复步骤(1)至步骤(7),直到找到倍式或者所有遍历完成.

(8)在倍式对应的最大统计量处的偏移量下,进行其他倍式的检测,得到倍式集合 $\{Q(x)\}$. 假设集合中包含 N_Q 个倍式.

(9)计算各偏移量下倍式判决的平均可信度(图 5),平均可信度最大的偏移位置作为粗同步位置返回. 判决可信度及平均可信度分别定义为:

$$c(Q(x),\Delta t) = \Phi\left(\frac{Z(Q(x),\Delta t) - \mu_1(Q(x))}{\sigma_1(Q(x))}\right) \tag{7}$$

$$\bar{c}(\Delta t) = \frac{1}{N_Q}\sum_{\{Q(x)\}} c(Q(x),\Delta t) \tag{8}$$

同步过程中采用了平均可信度最大准则,即在同步位置处倍式判决的可信度应达到峰值. 由式(7)可知,判决可信度位于区间(0,1)内. 在加性 Gauss 白噪声信道中,可采用不同帧的匹配滤波数据降低新构造序列的误码率[11]. 因此,仿真验证中假设误码率为 10^{-3},其他仿真条件与无噪声情况相同,不同情况下的仿真结果见表 2. 为加快算法收敛速度,步骤(8)使用了步骤(7)中倍式对应最大统计量处的偏移量,同时此做法可能会造成算法陷入局部最优解,无法完全检测到测试集中所有倍式,更加稳健的方法中应重复步骤(1)至步骤(7)搜索倍式集合. 在完成初始同步后,同样需要结合帧结构信息对解扰数据进行精确同步.

表 2 含噪情况下帧同步仿真结果

码型	帧长 N_b	反馈多项式	初始状态	估计值偏差
Hamming (7,4)	700	$1+x^2+x^3+x^4+x^8$	$[1,\mathbf{0}_6,1]$	0
		$1+x^3+x^4+x^6+x^9$	$[1,\mathbf{0}_2,1,\mathbf{0}_2,1,0,1]$	7
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\mathbf{0}_2,1,\mathbf{0}_3,1]$	7
BCH (7,4)	700	$1+x^2+x^3+x^4+x^8$	$[1,\mathbf{0}_6,1]$	-5,0,1,2,9
		$1+x^3+x^4+x^6+x^9$	$[1,\mathbf{0}_2,1,\mathbf{0}_2,1,0,1]$	-7,-6,0,1,7
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\mathbf{0}_2,1,\mathbf{0}_3,1]$	2
Hamming (7,4)	1400	$1+x^2+x^3+x^4+x^8$	$[1,\mathbf{0}_6,1]$	-7
		$1+x^3+x^4+x^6+x^9$	$[1,\mathbf{0}_2,1,\mathbf{0}_2,1,0,1]$	-14,-7,0
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\mathbf{0}_2,1,\mathbf{0}_3,1]$	0
BCH (7,4)	1400	$1+x^2+x^3+x^4+x^8$	$[1,\mathbf{0}_6,1]$	2,9
		$1+x^3+x^4+x^6+x^9$	$[1,\mathbf{0}_2,1,\mathbf{0}_2,1,0,1]$	-13,-6,1
		$1+x+x^2+x^3+x^5+x^6+x^{10}$	$[1,1,1,\mathbf{0}_2,1,\mathbf{0}_3,1]$	-6

注:$\mathbf{0}_n$ 表示 $1\times n$ 的全 0 向量$[0\ 0\ \cdots\ 0]$.

5 基于 Walsh-Hadamard 变换的计算方法

基于倍式搜索的扰码反馈多项式重建算法,其计算复杂度主要体现在搜索空间大小,以及检测统计量的计算上. 遍历所有可能偏移量 Δt 的过程,使得盲同步算法复杂度成倍增加,因此,提出基于 Walsh-Hadamard

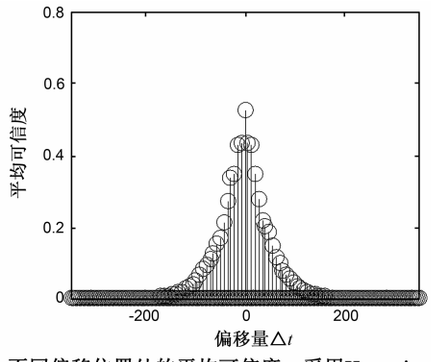

图5　不同偏移位置处的平均可信度，采用Hamming(7,4)编码，N_b=700，反馈多项式为$1+x^2+x^3+x^4+x^8$

变换的计算方法,以提高算法运算效率.

文献[14]在讨论“利用 Walsh 函数解二元域方程组”的应用时指出,Walsh-Hadamard 变换后谱系数的物理意义可表示为使方程组成立的个数与不成立个数之差. 因此,可基于 Walsh-Hadamard 变换进行检测统计量 Z 的计算.

Hadamard 矩阵 $\boldsymbol{H}_m$ 中任意元素 $h_{u,v}$ 的取值可表示为 $h_{u,v}=(-1)^{\boldsymbol{u}_u\boldsymbol{v}_v^{\mathrm{T}}}$,其中 $\boldsymbol{u}_m$ 和 $\boldsymbol{v}_m$ 分别为行号 u 和列号 v 的二进制行向量表示,不足 m 维时向前补零[15]. 2^m 维行向量 $\boldsymbol{a}$,经 Walsh-Hadamard 变换为 2^m 维行向量 $\boldsymbol{b}$,可表示为 $\boldsymbol{b}=\boldsymbol{a}\boldsymbol{H}_m$.

使用 Walsh-Hadamard 变换方法,仅需要进行一次原数据的统计,即构造向量 $\boldsymbol{a}$ 的过程. 这样可以节省在算法遍历过程中式(3)和式(6)计算 z_t 的时间,代价是需要计算 Hadamard 矩阵中特定元素的值. 但 Hadamard 矩阵中元素的取值是固定的,可通过查表方式获得,因此可以忽略计算 Hadamard 矩阵中元素值的复杂度. 鉴于解算问题的规模(表征为 D,如:50),构造向量 $\boldsymbol{a}$ 时将出现大量的0元素,所以建立位置-频次(u-f_u)字典以节省存储空间和提高运算速度. 不同的倍式对应 Hadamard 矩阵中不同的列,遍历字典即可计算检测统计量 Z. 结合 Walsh-Hadamard 变换的物理意义和统计量 Z 的表达式,可得到基于 Walsh-Hadamard 变换计算 Z 的方法如下:

(1)将生成序列$\{r_t\}$按长度 D 进行有重叠连续分组,并进行十进制转换,即将 $r_t r_{t+1}\cdots r_{t+D-1}$ 转换成十进制数,N_f 个数据将生成 N_f-D+1 个十进制数.

(2)用这 N_f-D+1 个十进制数构造位置-频次(u-f_u)字典(对应矢量 $\boldsymbol{a}$ 中的位置 u 和元素值 f_u,即将矢量 $\boldsymbol{a}$ 中第 u 个元素的所在位置标记为 $u-1$,第 u 个元素的取值等于 $u-1$ 在 N_f-D+1 个十进制数中出现的次数,$1\leqslant u\leqslant 2^D$).

(3)多项式 $Q(x)=1+x^{i_1}+\cdots+x^{i_{d-1}}$ 对应 2^D 阶 Hadamard 矩阵的第 v 列,其中 $v-1$ 等于 $Q(x)$ 的二级制表示(图6)对应的十进制数值,$1\leqslant v\leqslant 2^D$.

$$\underbrace{1\,0\cdots0\,1\,0\cdots0\,1}_{\text{第 } i_{d-1}\text{ 位}\qquad\qquad\text{第 } i_j\text{ 位}\qquad\qquad\text{第 0 位}}$$

图6　$Q(x)=1+x^{i_1}+\cdots+x^{i_{d-1}}$的二进制表示

(4)遍历字典进行累和,计算检测统计量

$$Z=\sum_{|u|}(-1)^{\boldsymbol{u}_u\boldsymbol{v}_b^{\mathrm{T}}}f_u \tag{9}$$

基于 Walsh-Hadamard 变换计算检测统计量时,对于不用阶数的倍式进行统计的 z_t 数量是一定的(N_f-D+1),避免了由于多项式变化需要重新计算不同假设下的均值和方差,从而可以使用固定的判决门限,和直接使用检测量的统计值表示判决可信度. 这样的代价是,统计数量减少,而降低判决的可靠性.

6　结束语

本文结合基于对偶码的扰码重建算法研究了帧同步盲识别问题. 首先,在无噪声情况下,利用扰码重建算法中检测统计量等于特定值的属性,可初步识别帧同步位置. 在完成粗同步后,即可重建扰码序列以解扰数据,再结合帧结构的特征实现精确同步位置的识别;其次,以平均判别可信度最大为帧同步识别准则,将无噪情况下的帧同步识别算法推广到含噪情况;最后,研究了基于 Walsh-Hadamard 变换的检测统计量计算方法,以构建标准化的计算模式,便于编程实现和降低算法复杂度. Walsh-Hadamard 变换方法,不适用于高误码率情况,可采用文献[11]中的多信息流算法降低数据误码率.

文中假设了对偶码参数已知,更具挑战性的问题是同时重建对偶码和扰码[1],利用重建算法中的判决过程,再结合上述同步框架,完成帧同步盲识别. 在使用自同步扰码的情况下,可结合自同步扰码重建算法[16],推广本文算法进行同步识别.

参考文献

[1] X B Liu, S N Koh, C C Chui, et al. A study on reconstruction of linear scrambler using dual words of channel encoder[J]. IEEE Trans Inf Forens Security, 2013, 8(3): 542 – 552.

[2] 牟青,魏平. 基于缺失数据模型的长码直扩信号的伪码估计[J]. 电子学报,2010,38(10):2365 – 2369.
Mou Qing, Wei Ping. Spreading waveform estimation of long-code DS-SS signals based on missing-data model[J]. Acta Electronica Sinica, 2010, 38(10): 2365 – 2369. (in Chinese)

[3] 谢春辉,程义民,陈扬坤. PN 序列估计与扩频隐藏信息分析[J]. 电子学报,2011,39(2):255 – 259.
Xie Chun-hui, Cheng Yi-min, Chen Yang-kun. PN sequence estimation and spread-spectrum steganalysis[J].

Acta Electronica Sinica,2011,39(2):255 – 259. (in Chinese)

[4] 任啸天,徐晖,黄知涛,等. 基于 Fast-ICA 同、异步系统短码 CDMA 信号扩频序列与信息序列盲估计[J]. 电子学报,2011,39(12):2726 – 2732.
Ren Xiao-tian, Xu Hui, Huang Zhi-tao, et al. Fast-ICA based blind estimation of spreading and information sequences of short-code CDMA signals in synchronous and asynchronous systems[J]. Acta Electronica Sinica,2011,39(12):2726 – 2732. (in Chinese)

[5] 任啸天,徐晖,黄知涛,等. 基于 Fast-ICA 的 CDMA 信号扩频序列优化盲估计[J]. 电子学报,2012,40(8):1532 – 1538.
Ren Xiao-tian, Xu Hui, Huang Zhi-tao, et al. Fast-ICA based optimize blind estimation of spreading sequence of CDMA signals[J]. Acta Electronica Sinica,2012,40(8):1532 – 1538. (in Chinese)

[6] M. Cluzeau. Reconstruction of a linear scrambler[J]. IEEE Trans Comput,2007,56(9):1283 – 1291.

[7] 罗向阳,沈利,陆佩忠,等. 高容错伪随机扰码的快速盲恢复[J]. 信号处理,2004,20(6):552 – 558.
Luo Xiang-yang, Shen Li, Lu Pei-zhong, et al. Fast blind restore of LFSR sequences with high error tolerance[J]. Signal Processing,2004,20(6):552 – 558. (in Chinese)

[8] 伍文君,黄芝平,唐贵林,等. 含错扰码序列的快速恢复[J]. 兵工学报,2009,30(8):1134 – 1138.
Wu W J,Huang Z P,Tang G L,et al. Fast recovery of interfered scrambling code sequence[J]. Acta Armamentarii, 2009,30(8):1134 – 1138. (in Chinese)

[9] 苏绍璟,伍文君,黄芝平,等. 含错 m 序列本原多项式的高阶统计测定算法[J]. 兵工学报,2010,31(12):1593 – 1598.
Su Shao-jing,Wu Wen-jun,Huang Zhi-ping,et al. Blind identification of the primitive polynomial of m-sequence with error using high-order statistic[J]. Acta Armamentarii,2010,31(12):1593 – 1598. (in Chinese)

[10] X B Liu, S N Koh, X W Wu, et al. Reconstruction of a linear scrambler with improved detection capability and in the presence of noise[J]. IEEE Trans Inf Forens Security, 2012,7(1):208 – 218.

[11] Yu Ma, Li-min Zhang, Hao-tong Wang. Reconstructing synchronous scrambler with robust detection capability in the presence of noise[J]. IEEE Trans Inf Forens Security,2015,10(2):397 – 408.

[12] T Johansson and F Jønsson. Improved fast correlation attacks on stream ciphers via convolutional codes[A]. Advances in cryptology [C]. Prague, Czech Republic: Springer-Verlag,1999. 347 – 362.

[13] Shaodan Ma, Xinyue Pan, Guang-Hua Yang, et al. Blind symbol synchronization based on cyclic prefix for OFDM systems[J]. IEEE Trans Veh Technol,2009,58(4):1746 – 1751.

[14] 游凌,朱中梁. Walsh 函数在解二元域方程组上的应用[J]. 信号处理,2000,16(增刊):27 – 30.
You Ling, Zhu Zhong-liang. The application of Walsh Function in Resolving of F(2) equations[J]. Signal Processing,2000,16(supplement):27 – 30. (in Chinese)

[15] N. Ahmed, K. R. Rao. Orthogonal Transforms for Digital Signal Processing[M]. 胡正名,陆传,译. 北京:人民邮电出版社,1979.

[16] 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.
Liao Hong-shu, Yuan Ye, Gan Lu. Novel blind reconstruction method for self-synchronized scrambler[J]. Journal on Communications, 2013, 34(1): 136 – 143. (in Chinese)

作者简介

马 钰 男,1986 年生于山西寿阳. 海军航空工程学院电子信息工程系博士生,助理工程师. 研究方向为综合电子战系统、非合作数字信号处理.
E-mail:my7202359@126.com

张立民(通信作者) 男,1966 年生. 海军航空工程学院教授,博士生导师. 研究方向为综合电子战系统与技术、军用仿真技术.
E-mail:iamzlm@163.com

王好同 男,1958 年生. 海军航空工程学院副教授,硕士生导师. 研究方为航空通信与导航.
E-mail:haotong_1958@126.com