

移位位反序列捕获算法

任国风¹, 吉江^{2*}, 田竹梅¹

(1. 忻州师范学院 电子系, 山西 忻州 034000; 2. 国家数字交换系统工程技术研究中心, 郑州 450002)

(* 通信作者电子邮箱 jijinjiang@sohu.com)

摘要:当捕获周期较长的序列时,传统的滑动相关捕获方式会消耗巨大的系统资源。为此提出位反向量和移位位反向量,使得由序列状态的试错结果可直接推断出后续序列状态的试错结果,从而避免重复的序列推算过程,提高滑动相关效率。随后通过证明控制状态的生成规律,节省了位反向量及移位位反向量的存储空间。据前述原理,设计出了移位位反序列捕获算法及其接收机,使得捕获复杂度从常规的 $O(n^2)$ 下降为 $O(n)$ 。

关键词:序列捕获; m 序列; 序列状态; 移位位反向量; 信息安全

中图分类号: TN911; TP309.7 **文献标志码:** A

Shifted bit inverse sequential acquisition algorithm

REN Guofeng¹, JI Jiang^{2*}, TIAN Zhumei¹

(1. Department of Electronics, Xinzhou Teachers University, Xinzhou Shanxi 034000, China;

2. China National Digital Switching System Engineering and Technological R&D Center, Zhengzhou Henan 450002, China)

Abstract: When the period of objective sequence is long enough, the traditional acquisition algorithm will consume a lot of system resource. The shifted bit inverse sequential acquisition algorithm was proposed, which could be utilized to deduce the trail-and-error results of following sequence state from the previous trail-and-error result. As a result, the complicated sequence shifting calculation was avoided. Then the rule of the control state was proved, which led to the storage space reduction of the bit inverse vector and shifted bit inverse vector. Finally, an acquisition system based on the theory mentioned above was designed, which could acquire sequence with high efficiency, and the complexity decreased from conventional $O(n^2)$ to $O(n)$.

Key words: sequential acquisition; m sequence; sequence state; shifted bit inverse vector; information security

0 引言

扩频通信系统利用了伪随机(Pseudo-Noise, PN)序列良好的自相关和互相关特性,不仅在军用通信系统、制导系统等军事技术领域中占有重要地位,而且在移动通信系统 WCDMA(Wideband Code Division Multiple Access)、CDMA2000(Code Division Multiple Access)、无线电测距/测速、导航以及目标探测等民用领域也得到了非常广泛的应用^[1]。扩频通信系统的窃听及同步均需要高性能的序列捕获算法^[2-3]。在同步过程对 PN 序列进行捕获即是首先要确定 PN 序列的相位^[4-5]。目前较为实用的是序列滑动相关捕获算法。

滑动相关捕获法基于滑动相关的思想,目前有关滑动相关捕获法的研究分为两个方向:

1) 主要着眼于研究一些捕获参数^[6],包括判决门限、捕获序列状态量等。文献[7-8]综合各种信道因素针对参数进行了讨论,并且提出了一些自适应参数计算法则;文献[9]分析了部分相关捕获算法在多径环境中的性能;文献[10]讨论了在乘性噪声和加性噪声环境中的相关捕获性能;文献[11]为直扩序列捕获设置自适应门限。

2) 借助于辅助的接收序列进行捕获。例如文献[12]针对长周期序列,采用部分序列尝试捕获重构;文献[13]中设计出一种串行接收机,主要利用辅助序列对初始状态进行修正,从而提高捕获速度;文献[14]通过建立预备的估计序列

协助后续序列并行捕获。

相关捕获法每次只对一个可能的初始状态与接收序列进行相关运算,所以当 PN 序列的周期巨大时,现有上述方法将无法实时进行捕获^[15]。所以如何设计序列计算结构,降低相关运算的复杂度是提高序列捕获性能的根本。

为此本文提出位反移位序列捕获算法。算法首先构造了位反向量和移位位反向量,这两个向量凭借序列控制状态刻画了两序列状态改变量的映射关系,因此算法可通过直接建立待捕获序列状态与后续序列状态间的误码对应关系,降低滑动相关运算的复杂度。为保证算法的实时性,降低接收机的存储空间,本文还推导、证明了序列控制状态的生成规律。最终算法可以通过查询移位位反向量表来实现低复杂度的序列捕获过程,将捕获复杂度从常规的 $O(n^2)$ 下降为 $O(n)$ 。

1 序列状态与的元素映射关系

移位位反向量表主要用于降低移位相关的复杂度,提高计算序列相关峰的速度。其主要思想是讨论序列状态改变后的后续状态变化关系。利用此关系建立序列相关的移位位反向量表,通过查表直接修改序列状态后续的状态,从而实现序列快速遍历相关。移位位反向量的基础是序列状态与元素间的映射关系,下面进行该映射关系的讨论。

在 F_2 域上,令待捕获 m 序列的生成多项式为 $f(D) = D^n + c_1 D^{n-1} + c_2 D^{n-2} + \dots + c_n (n > 0)$;周期为 $P = 2^n - 1$;线

收稿日期:2013-03-05;修回日期:2013-05-31。 基金项目:忻州师范学院院级基金项目(201016)。

作者简介:任国风(1979-)女,山西忻州人,讲师,硕士,主要研究方向:现代编码理论、计算机网络安全;吉江(1983-)男,山西忻州人,博士研究生,主要研究方向:无线宽带通信、物理层安全;田竹梅(1980-)女,山西原平人,讲师,硕士,主要研究方向:自组织网络、盲信号处理。

性反馈移位寄存器的初始相位(状态)为 $S_0 = (a_0, a_1, \dots, a_{n-1})^T$, 其中 a_n 为序列 n 时刻的值。则它的产生满足递推关系如下:

$$a_{n+i} = c_1 a_{n+i-1} + c_2 a_{n+i-2} + \dots + c_n a_i \quad (1)$$

上述关系也可用状态转移矩阵表示, 显然, 上述递推关系的状态转移矩阵为

$$T = \begin{bmatrix} 0 & 0 & 0 & \dots & c_1 \\ 1 & 0 & 0 & \dots & c_2 \\ 0 & 1 & 0 & \dots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 1 & \dots & c_n \end{bmatrix} \quad (2)$$

则 $S_{j+i}^T = S_j^T T^i$ 。

由 m 序列的产生规律得, 第 j 个状态为

$$S_j^T = (a_0, a_1, \dots, a_{n-1}) T^j \quad (3)$$

令

$$(X_{0+j}, X_{1+j}, \dots, X_{n-1+j}) = T^j \quad (4)$$

其中: $X_{k+j} = (x_{k+j,0}, x_{k+j,1}, \dots, x_{k+j,n-1})^T$, $x_{k+j,i} \in \{0,1\}$, $k \in \{0,1, \dots, n-1\}$, 因此有

$$S_j^T = (a_j, a_{j+1}, \dots, a_{n-1+j}) = (a_0, a_1, \dots, a_{n-1}) \cdot (X_{0+j}, X_{1+j}, \dots, X_{n-1+j}) \quad (5)$$

即

$$a_j = (a_0, a_1, \dots, a_{n-1}) \cdot X_j \quad (6)$$

在式(6)中, X_j 表示初始序列状态 S_0^T 和后续序列元素 a_j 之间的生成关系, 称之为控制状态。控制状态有如下定理成立:

定理 1 对于任意的线性反馈移位寄存器 (Linear Feedback Shift Register, LFSR) 序列, 如果其生成多项式为 $f(D)$, 则对应的控制状态中元素 $x_{i,k}$ 随 i 变化也为 LFSR 序列, 并且此序列的生成多项式仍为 $f(D)$ 。

证明 设 $S = (a_0, a_1, \dots, a_{n-1}, \dots)$ 是 LFSR 序列, S_j 为其第 j 个状态, 生成多项式为 $f(D) = D^n + c_1 D^{n-1} + c_2 D^{n-2} + \dots + c_n$, 则它的产生满足如下递推关系:

$$a_{n+i} = c_1 a_{n+i-1} + c_2 a_{n+i-2} + \dots + c_n a_i \quad (7)$$

根据式(5)可知

$$a_j = (a_0, a_1, \dots, a_{n-1}) \cdot T^j \cdot (0, 0, \dots, 1)^T \quad (8)$$

又因为

$$a_j = a_0 \cdot x_{j,0} + a_1 \cdot x_{j,1} + \dots + a_{n-1} \cdot x_{j,n-1} = (a_0, a_1, \dots, a_{n-1}) \cdot (x_{j,0}, x_{j,1}, \dots, x_{j,n-1})^T \quad (9)$$

由式(8)、(9)右端相等得:

$$x_{j,k} = (0, 0, \dots, 1, \dots, 0)^T \cdot T^j \cdot (0, 0, \dots, 1)^T \quad (10)$$

其中: $k = 1, 2, \dots, n$, 行向量中的 1 在第 k 位上。

与式(8)相比较可得控制状态中元素 $x_{i,k}$, 随 i 变化也为 m 序列, 并且此序列的生成多项式为 $f(D)$ 。

根据此定理可知, 对于某序列状态 S_0^T 和后续序列元素 a_j , 其对应的控制状态 X_j 在一个序列周期内随 j 的变化而不同, 即 S_0^T 和 a_j 之间存在 X_j 的映射关系。按照该定理就可以得到映射关系 X_j 。

2 移位位反捕获理论

下面讨论差异序列状态在移位寄存器移位相同次数后产生的序列状态间的关系。把式(6)改写成如下:

$$S_j = (a_j, a_{j+1}, \dots, a_{n-1+j})^T = (Y_{0+j}, Y_{1+j}, \dots, Y_{n-1+j}) \cdot (a_0, a_1, \dots, a_{n-1})^T \quad (11)$$

其中: $(Y_{0+j}, Y_{1+j}, \dots, Y_{n-1+j}) = (X_{0+j}, X_{1+j}, \dots, X_{n-1+j})^T$; $Y_{k+j} = (y_{k+j,0}, y_{k+j,1}, \dots, y_{k+j,n-1})^T$, $y_{k+j,i} \in \{0,1\}$, $k \in \{0,1, \dots, n-1\}$ 。将式(11)写成求和形式如下:

$$S_j = (a_j, a_{j+1}, \dots, a_{n-1+j})^T = \sum_{k=0}^{n-1} Y_{k+j} \cdot a_k \quad (12)$$

令与 S_0 第 i 个元素存在差异的另一初始序列状态为 $S_0' = (a_0, a_1, \dots, \bar{a}_i, \dots, a_{n-1})^T$, 其中元素 \bar{a}_i 表示与 a_i 不同(互反)。则有

$$S_j' = (a_j', a_{j+1}', \dots, a_{n-1+j}')^T = (Y_{0+j}, Y_{1+j}, \dots, Y_{n-1+j}) \cdot (a_0, a_1, \dots, \bar{a}_i, \dots, a_{n-1})^T = \sum_{k=0, k \neq i}^{n-1} Y_{k+j} \cdot a_k + Y_{i+j} \cdot \bar{a}_i = \sum_{k=0}^{n-1} Y_{k+j} \cdot a_k + Y_{i+j} = S_j + Y_{i+j} \quad (13)$$

根据式(13)可知, 当 S_0 中第 i 位取反后, 其对应的 j 步移位后的状态 S_j' 为 S_j 状态与 Y_{i+j} 之和。进一步可知当 $S_0' = (a_0, a_1, \dots, \bar{a}_i, \dots, \bar{a}_i, \dots, a_{n-1})^T$ 时, 有

$$S_j' = S_j + Y_{i+j} + Y_{i+j} \quad (14)$$

结论 当序列初始状态 S_0 中分别在第 i_m ($1 \leq m \leq M$) 位上的 M 个元素取反后, 其后续第 j 个序列状态 S_j' 为:

$$S_j' = S_j + \sum_{m=1}^M Y_{i_m+j} \quad (15)$$

$\Omega = \sum_{m=1}^M Y_{i_m+j}$ 表明在初始状态某些位发生取反后需要对原后续第 j 个序列状态所做的调整情况, 所以称其为移位位反向量。

根据上述理论分析, 下面通过生成多项式为 $f(D) = D^5 + D^3 + D^2 + D + 1$ 的伪随机序列对移位位反序列捕获算法进行说明。如图 1 所示对于序列第 6 个元素的控制状态 $X_6 = (x_{6,0}, x_{6,1}, \dots, x_{6,n-1})^T = (1, 0, 1, 1, 1)^T$, 其中有抽头的 $x_{6,k}$ 对应“1”, 没有的对应“0”。这表明第 6 个元素 a_6 可以通过初始初始状态的 a_0, a_2, a_3 和 a_4 模加生成, 而与 a_1 无关; 同样第 7 个元素 a_7 可以通过初始初始状态的 a_0, a_1, a_2 模加生成, 而与 a_3 和 a_4 无关。这样便建立起后续序列元素与初始状态 S_0 的关系。

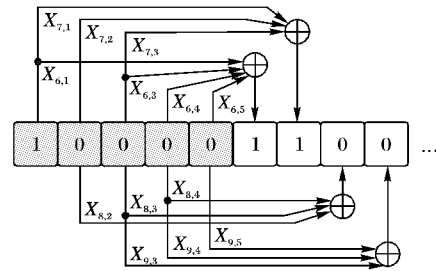


图 1 控制状态示意图

通过控制状态可以得到前 n 个移位位反向量, 而全部 $2^n - 1$ 种位反向量对应的移位位反向量可由前 n 个移位位反向量组合模加计算得出。生成多项式为 $f(D) = D^5 + D^3 + D^2 + D + 1$, 对于后续第 11 个状态的控制位反向量见表 1。

利用位反向量和移位位反向量进行序列估计的原理如图 2 所示, 序列的生成多项式为 $f(D) = D^5 + D^3 + D^2 + D + 1$ 。当接收到含有误码(误码在图中用深灰色表示)的伪随机序列时, 需要估计出目标序列状态的正确值。首先猜测可能的误码位, 在图 2 中猜测第 2、3 两位错误, 其对应的位反向量为 $(0, 1, 1, 0, 0)^T$ 。接收到的待捕获目标序列状态为 $(1, 1, 1, 0, 0)^T$, 其后续序列按照生成多项式可得为 $(1, 1, 1, 0, 0, 0, 1,$

0,1,0,1,1,0,1,0)^T。于是按照错误的待捕获状态,其第 11 个状态为(1,1,0,1,0)^T。按照图 2 左下所示,将位反向量与待捕获状态进行异或得到序列状态(1,0,0,0,0)^T,其对应的后续第 11 个状态为相应的移位位反与原后续状态(1,1,0,1,0)^T异或的结果,即为(0,0,1,1,1)^T。这与原接收的第 11 个状态(0,0,0,1,1)^T相近,按照 m 序列的伪随机性可判知所猜测的序列结果正确,得到正确的捕获结果(1,0,0,0,0)^T。若此次猜测错误,则进行其他位的猜测并进行查询移位位反向量表操作。

表 1 第 j 个状态的辅助表

序号	位反向量 (n 维)	第 11 个状态的移位位反向量 Ω(n 维)
0	(00000)	(00000)
1	(10000)	(00111)
2	(01000)	(10011)
3	(00100)	(01110)
4	(00010)	(10000)
5	(00001)	(01111)
⋮	⋮	⋮
10	(01100)	(11101)
⋮	⋮	⋮
31	(11111)	(00101)

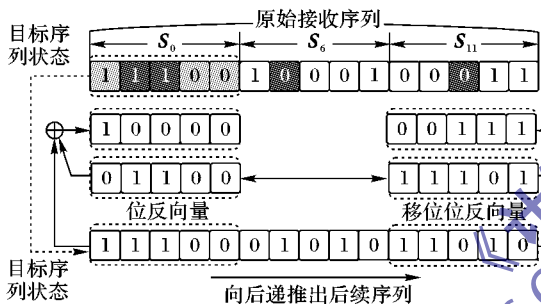


图 2 移位位反序列估计原理图

3 移位位反的序列捕获算法

通过上文讨论可知,移位位反向量表内包含待捕获状态变化后,后续序列变化的规律信息。因此如果在序列捕获的本地接收机中预存移位位反向量表,则必然可以提高捕获速度。为此利用移位位反向量表设计如图 3 的序列捕获接收机结构。

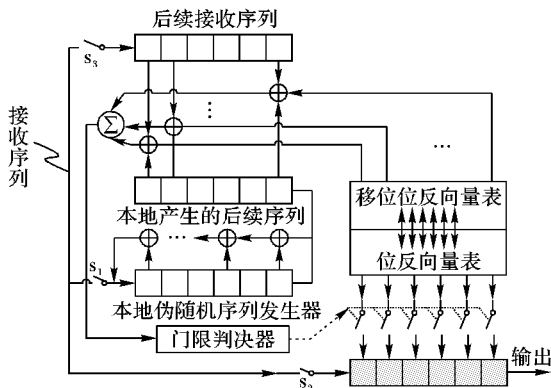


图 3 移位位反捕获算法的接收机结构原理图

接收机主要由三部分组成:1)本地伪随机序列发生器,用来产生后续伪随机序列;2)移位位反向量表,预存了序列捕获的移位位反信息;3)存储有本地产生的后续序列的移位寄存器。其中 2)和 3)两部分共同构成了快速取反单元。整

个接收机的工作流程如下:

- 1)开关 s_1 和 s_2 闭合,将接收序列(0-1 序列)分别输入到本地伪随机序列发生器和输出端的寄存器中,作为待捕获的序列状态。
- 2)本地伪随机序列发生器产生本地后续的第 j 个序列状态。
- 3)开关 s_3 闭合, s_1 和 s_2 断开,将接收到的后续第 j 个序列状态移入移位寄存器中。
- 4)移位位反向量表中遍历第 j 个修正状态,并从上方输出后与本地以及接收到的第 j 个序列状态进行模加求和运算。
- 5)将运算结果与判决门限相比较,如果大于门限则输出结果;否则执行第 4)步,继续遍历。

4 算法的性能测试与分析

按照上述实现方案对算法从两方面进行性能分析:1)算法的实现复杂度分析。从理论上对算法复杂度进行初步分析,随后利用实际测试结果与理论结果进行对比。2)算法对含错序列的捕获能力分析。目前移位位反序列捕获算法对于 CDMA2000 下的含错长码序列捕获能力有限,当误码较多时需要一定的时间才能成功实现捕获,所以结合实时性对其捕获能力进行分析可以明确算法的捕获能力。根据上第二章的分析,CDMA2000 的 PN 序列发生器的生成多项式为:

$$f(x) = x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1 \quad (12)$$

在整个相关机制算法的捕获过程中,模加运算为算法的主要开销,因此可以用模加运算次数来衡量算法的复杂性。设目标序列状态长度为 n ,后续长度为 $k \cdot n$ 的序列状态作为判决状态,并且序列发生器具有 $n/2$ 个反馈抽头。如果有误码的序列状态中恢复目标序列状态,由于未知序列状态的误码情况共有 $2^n - 1$ 种,所以常规相关捕获的思路要全部遍历判决这 $2^n - 1$ 种情况需要模加运算 $0.5k \cdot n^2 \cdot (2^n - 1)$ 次;而按照文中提出的位反移位相关捕获算法,模加运算的次数为 $k \cdot n \cdot (2^n - 1)$ 次。可见对于单次相关判决,运算次数从 $0.5 \cdot k \cdot n^2$ 降至 $k \cdot n$,即算法复杂度从 $O(n^2)$ 降为 $O(n)$ 。对于长周期序列捕获来说, n 的取值较大,其算法实时性的优势更加明显。

图 4 为移位位反序列捕获算法在不同信噪比情况下的最大时间开销,与其相比较的是常规的遍历捕获算法。从图中可以看到,当信噪比都为 0 时,两种算法的时间开销相同,但随着误码增多,移位位反算法的耗时明显较少。传统的相关机制遍历捕获算法在图中可近似拟合二次曲线,而移位位反序列捕获算法可拟合一条直线。所以实际的测试结果基本与理论分析结果相一致。

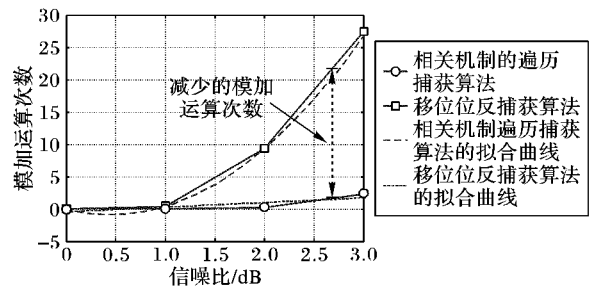


图 4 移位位反算法与常规遍历算法耗时对比

序列捕获算法的另一项重要指标是序列经捕获后的误码

率,本文首先在高斯加性信道利用移位位反算法和常规的遍历算法对式(12)所示的序列进行捕获。信噪比分布范围为 $-30 \sim 0$ dB,捕获长度分别为单倍序列状态(42个序列)、双倍序列状态(84个序列)、三倍序列状态(126个序列)、四倍序列状态(168个序列)。仿真结果如图5所示(括号内数字表示捕获长度为单倍序列状态的倍数),从图中可以看出两种算法在四种序列长度下的误码率曲线均基本重合。结合图4可知,移位位反算法在保证捕获性能(误码率)的同时,提高了捕获速度。

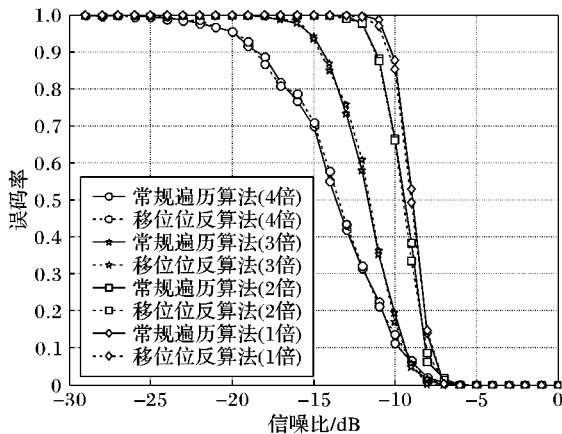


图5 高斯白噪声信道下两算法的捕获性能对比

同样依照加性高斯信道下的仿真条件,在瑞利衰落信道下仿真算法的误码性能。仿真结果如图6所示,其中将纵坐标的误码率取对数,以便于观察误码性能。类似地,可以看出两种算法在四种序列长度下的误码率曲线均基本重合,进一步证明移位位反算法与传统遍历捕获算法性能相同,但具有较高的捕获速度。

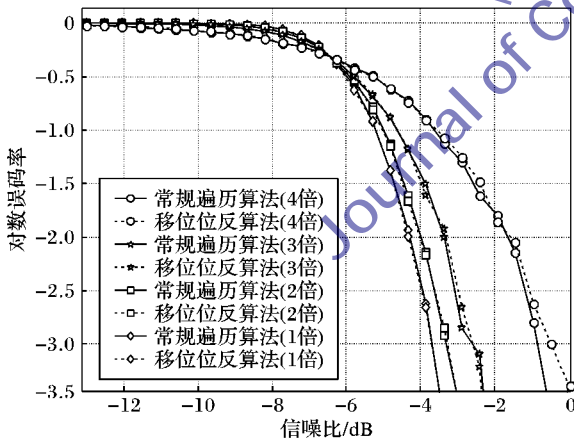


图6 瑞利衰落信道下两算法的捕获性能对比

由于引入了控制状态,移位位反序列捕获算法可以利用较小的存储空间快速实现捕获。原本算法需要大量的空间存储位反向量和移位位反向量,从而以存储空间换取序列捕获速度。以式(12)所示的序列为例,每个向量需要42 b存储空间,通常采用8 B存放,当信噪比低导致每个序列状态中误码平均为3个时,需要的存储空间为 $2 \times 42^3 \times 8 = 1.185408$ (MB),随着待捕获序列中的误码数量增多,需要本地存储空间增大。为了在此算法中减少本地存储空间,本文通过理论分析证明了移位位反向量的生成规律(见文中定理1)。利用定理中描述的规律可以实时生成全部本地所存储的向量,此时本地所需的存储空间降为 $42 \times 8 = 336$ (B),最终使得移位位反序列捕获算法所需的存储空间较小。

5 结语

本文提出了移位位反序列捕获算法,算法的主要思想是在序列捕获的试错过程中,通过建立序列状态间的改变量对应关系,直接对前次试错结果进行修改,以得到下一次试错结果,从而降低序列捕获过程的复杂度。在研究过程中,发现序列状态的改变量对应关系可以用具有一一映射关系的移位向量和移位位反向量来表示,从而依据该关系设计出移位位反序列捕获算法,使得捕获性能相同的基础上,复杂度从常规的 $O(n^2)$ 下降为 $O(n)$ 。为进一步提高序列捕获效率,在后续的研究中需要对每次试错结果对后续试错的启发式信息进行挖掘,以减少试错次数,降低捕获时间。

参考文献:

- [1] 刘家胜,黄贤武,朱灿焰,等.基于m序列整数调制和置乱的图像加密算法[J].计算机应用,2007,27(1):118-121.
- [2] 吉江,黄开枝,金梁,等.可控单积累状态序列捕获算法[J].中国科学:F辑,2009,39(10):1112-1124.
- [3] 花文昭,赵龙,韩文报.椭圆曲线线性同余序列的格攻击[J].计算机应用,2011,31(S2):97-99.
- [4] YANG L-L, HANZU L. Acquisition of m-sequences using recursive soft sequential estimation [J]. IEEE Transactions on Communications, 2004, 52(2):199-204.
- [5] LIU Y Z, PAN Y H, YAO F Q. A modified adaptive filtering acquisition method for PN code with data modulation [J]. IEEE Communications Letters, 2011, 15(8): 869-871.
- [6] SHEN F, GAI M, HE R. PN code acquisition using locally optimum statistics in blind channels [C]// Proceedings of the 2011 3rd International Conference on Advanced Computer Control. Piscataway: IEEE, 2011: 337-340.
- [7] 冯富强,陈鹏举,武传华,等.低信噪比条件下DS信号的检测和参数估计[J].通信学报,2002,23(9):63-67.
- [8] KIM C-J, LEE H-J, LEE H-S. Adaptive acquisition of PN sequences for DSSS communications [J]. IEEE Transactions on Communications, 1998, 46(8):993-996.
- [9] DU X H, ZHANG T Q, GAO Y S, et al. Analysis on PN code acquisition performance in DS-SS over multipath environment [C]// Proceedings of the 3rd International Congress on Image and Signal Processing. Piscataway: IEEE, 2010, 9: 4349-4353.
- [10] SHEN F, GAI M, WANG Z-L, et al. Code acquisition using the locally optimum test statistics in both multiplicative and additive noises [C]// Proceedings of the 2011 IEEE International Conference on Mechatronics and Automation. Piscataway: IEEE, 2011:1174-1178.
- [11] YEOM S, JUNG Y, LEE S. An adaptive threshold technique for fast PN code acquisition in DS-SS systems [J]. IEEE Transactions on Vehicular Technology, 2011, 60(6): 2870-2875.
- [12] LI H, LU M, FENG Z. Partial-correlation-result reconstruction technique for weak global navigation satellite system long pseudo-noise-code acquisition [J]. IET Radar Sonar Navigation, 2011, 5(7): 731-740.
- [13] SALIH M, TANTARARATANA S. A closed-loop coherent PN acquisition system with a pre-loop estimator [J]. IEEE Transactions on Communications, 1999, 47(9):1394-1405.
- [14] DELVA J G R, HOWITT I. PN acquisition for DS/SS using a preloop parallel binary search phase estimator and a closed-loop selective search subsystem [J]. IEEE Transactions on Wireless Communications, 2004, 3(2):408-417.
- [15] 钟锦,王大刚.图像信息安全处理的矩阵序列的周期性性质[J].计算机应用,2012,32(9):2592-2594.