局部跳频序列特性分析

张世杰,全厚德
(军械工程学院,河北 石家庄 050003)

摘 要:为了更全面的对跳频序列特性进行验证,针对实际跳频通信中仅使用局部跳频码序列的特点,提出了对局部跳频序列进行特性分析的方法。该方法在全周期跳频序列特性分析的基础上进行改进和补充,分别从动态性能、游程特性、频隙滞留和抗破译性等方面,对局部跳频序列进行分析,并给出各项性能指标的评价方法,为跳频序列的设计和检验提供了参考依据,规范了评价标准。同时,对 256 频点、截断长度为 10^6 的 m 序列的局部序列特性进行分析验证,对 m 序列的性能进行了较为全面的评价。

关键词:局部跳频序列;性能测试;动态特性;抗破译性
中图分类号:TN914.4 **文献标识码**:A **文章编号**:1673-629X(2012)09-0169-04

Analysis of Partial Frequency-hopping Sequence

ZHANG Shi-jie, QUAN Hou-de
(Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: It proposed a method of partial FH sequence analysis in consideration of the using of partial sequence in FH communications for testing the performance of FH sequence comprehensively. The method is improved and replenished based on the property analysis of the whole sequence which embrace the dynamic property, run path, anti-forecast and so on. The analysis is provided for devising and testing FH sequence. To take partial m sequence ($q=256, L=10^6$) for an example, the property of the partial FH sequence is analyzed and verified, and the performance of m sequence is estimated comprehensively.

Key words: partial FH sequence; performance test; dynamic property; anti-forecast

0 引 言

跳频通信设备通过控制跳频码发生器,产生频率跳变的射频信号,躲避敌方干扰,接收方通过相关监测方法获取跳频信号,实现收发双方抗干扰通信。跳频序列是用来控制载波频率跳变的多值序列,在很大程度上影响了跳频通信系统的性能,并且通常要求跳频序列具有良好的动态特性、高复杂度、多址性能和较宽的频隙间隔等。

目前,对跳频码序列性能的测试主要为全序列周期的测试[1~6],很少关注局部跳频码序列的性能。然而在一次跳频通信过程中,用户实际使用的跳频序列,仅仅是整个序列周期中很短的一部分,例如,SINCGARS-V^{2}甚高频跳频电台,序列周期达到 $2^{32}-1$,对于每秒 500 跳的中速跳频,持续通信 1h 大约使用了跳频码序列的 0.0417%。跳频序列的某些性能在全周期时满足要求,在局部序列并不能满足要求,势必将影响跳频通信的效率。基于这个事实,在进行跳频序列设计时,不仅要考虑整个序列周期的跳频码序列的性质,更应该考虑局部跳频序列的性质,使跳频序列的研究对工程操作更有指导意义。

收稿日期:2012-01-10;**修回日期**:2012-04-19
基金项目:国防预研基金资助项目(513270203)
作者简介:张世杰(1988-),男,河南濮阳人,硕士研究生,研究方向为跳频通信理论与技术;全厚德,博士,教授,主要研究方向为情报指挥系统、通信设备性能测试。

1 动态特性

跳频序列一般具有较长的周期,需要满足截断后实际应用的序列段尽可能保持平衡,并满足汉明自(互)相关特性的要求。局部跳频序列的这种平衡性和汉明相关性称为动态特性[7]。

1.1 平衡性

为使跳频系统具有良好的抗干扰性能,应使各频率在截断后的跳频序列段中出现的次数基本相同,这就是序列的动态平衡性。对于一段长度为 L 的 q 元跳频码伪随机序列要满足均匀分布的要求,即在 q 个频率点上跳频码出现的几率应相同。采用标准的 χ^2 检验法来检验衡量跳频序列的均匀程度。

均匀性判据:若 q 元中的元素 i 出现的次数为 f_i,则

$$\chi^2 = \sum_{i \in GF(q)} \frac{(f_i - L/q)^2}{L/q}$$

当计算得到的 χ^2 值小于指定的显著水平(例如 5%)下的 χ^2 值时,可以认为 f_i 以值 L/q 均匀分布的假设为真,否则为假。

仿真模型:建立 GF(2)上的 L-G 模型,它通过连续抽头,将 n 级连续的线性移位寄存器的状态与初始密钥(地址码)进行位异或,产生具有平衡性和最佳汉明相关性能的跳频序列。使用 25 位移位寄存器为例,抽头位置选为(25,3,2,1),则序列周期 $2^{25}-1$,频率集数目 256。

为了测试局部跳频序列码平衡性,从构造的长周期跳频中随机选取 10 条不重复序列($L = 10^6$)。图 1 示出了此局部序列均匀性测试的 χ^2 统计与 $\chi^2_{255}(0.05)$ 对比结果。由统计结果看出, m 序列基本通过了均匀性测试,具有较良好的动态平衡性。

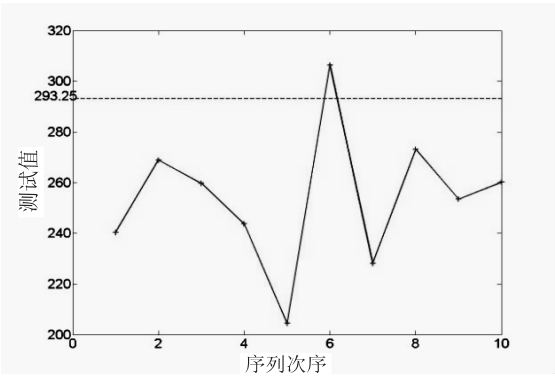

图 1 局部序列平衡性测试结果

1.2 汉明自(互)相关性

汉明相关性包括汉明自相关和汉明互相关,对跳频序列的同步性能和多址组网性能有重要影响。由于跳频序列的长周期性,不存在周期循环使用的情况,故应用周期汉明相关性描述局部跳频序列的特性是没有意义的,这里引入新的汉明相关定义[8]。长度为 L 的 q 元伪随机序列 $S_u = \{s_u(j)\}$ 和截断长度为 M 的 q 元伪随机序列 $S_v = \{s_v(j)\}$ 在相对时延 τ 时的汉明相关定义为:

$$H_{S_uS_v} = \sum_{j=0}^{M-1} h[s_u(j), s_v(j+\tau)], \quad 0 \leqslant \tau \leqslant L - M + 1$$

局部跳频序列的汉明自相关最大旁瓣为:

$$H(S_u) = \max_{0<\tau<L-M+1} \{H_{S_uS_u}(\tau)\}$$

$H(S_u)$ 是序列 S_u 与时延 τ 时的序列最大的重合次数,汉明自相关特性影响通信系统的抗多径干扰能力。当该跳频码作为同步引导码时,同样将影响该系统的同步性能。

局部跳频序列汉明互相关峰值定义为:

$$H(S_u, S_v) = \max_{0<\tau<L-M+1} \{H_{S_uS_v}(\tau)\}$$

$H(S_u, S_v)$ 是序列 S_u 与序列 S_v 在时延 τ 的最大重合次数,局部跳频序列的汉明互相关特性影响系统的多址组网能力和抗干扰能力。

下面对局部跳频序列码相关性进行测试,从构造的长周期跳频中随机选取 10 条不重复序列, $L = 10^6$。表 1 列出了部分局部序列汉明相关性统计结果。由统计结果看出,局部序列的汉明相关值保持平稳,且维持在较低水平(相关系数约为 0.004),说明该序列动态相关性能良好。

表 1 局部序列汉明自(互)相关性统计结果

序列	1	2	3	4	5	6	7
$H(S_u)$	4220	4184	4197	4198	4183	4206	4189
$H(S_u,S_v)$	4096	4111	4103	4089	4108	4111	4098

2 宽间隔、频隙滞留和游程特性

2.1 宽间隔

跳频通信通过频点的不间断跳变方式来躲避敌方的干扰信息,倘若在一个频点驻留时间过长,则容易受到各种干扰。因此,需要对跳频序列进行宽间隔的设计处理,这样有利于对抗部分频带干扰、跟踪干扰和多径衰落等多种干扰。

长度为 L 的 q 元伪随机序列 $S = \{s(j)\}$, $s(j)$ 、$s(j+1)$ 为两个相邻跳频码,满足关系式:

$$d + 1 \leqslant s(j) - s(j+1) \leqslant q - d + 1$$

则称该跳频序列的最小频隙间隔为 d ,测试较为简单,这里不再赘述。本仿真方案使用 L-G 模型构造的跳频序列不具备宽间隔特性,但可以通过对偶频带法和宽间隔处理等方法[9]实现跳频序列宽间隔,这需要足够的频谱资源支持。

2.2 频隙滞留

频隙滞留是指跳频系统在相邻的两跳或多跳使用频率集中的同一个频率,主要由跳频码序列产生器的结构和跳频码的游程特性产生。如果信号在某一频隙上停留相当长的时间,则易被非法接收机检测、截获,从而实施跟踪或转发式干扰。

若长度为 L,均匀分布的 q 元跳频码伪随机序列,频隙滞留的数学期望为 L/q。频隙滞留判决:对于每一条长度为 L 的 q 元跳频码伪随机序列,测试序列长度内某一频点的频隙滞留值 p_j。共进行 k 条序列的测试,其中有

$$\chi^2_{k-1} = \sum_{j=1}^{k} \frac{(p_j - L/q)^2}{L/q}$$

χ^2_{k-1} 的值小于指定的显著水平(例如 5%)下的自由度为 $k-1$ 的 χ^2 值时,则它以值 L/q 的均匀分布可信,称频隙滞留特性合格,否则为不合格。

为了测试局部跳频序列码频隙滞留特性,从构造

的长周期跳频中随机地选取 30 条不重复序列($L = 10^6$),分别对 256 个频点进行频隙滞留测试。图 2 示出了局部序列对256 个频点的频隙滞留测试χ^2 统计与 $\chi^2_{255}(0.05)$ 对比结果[10]。由统计结果看出,局部跳频序列基本通过了频隙滞留特性测试,但仍有部分频隙不满足频隙滞留标准,需要进一步改进。

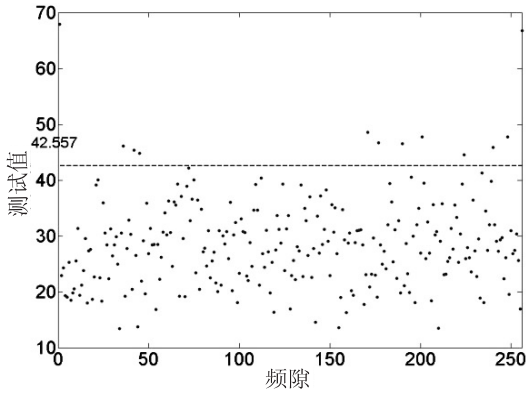

图 2　频隙滞留测试结果

2.3　游程特性

游程是指跳频系统在连续多跳使用频率集中的同一个频率的次数。一个跳频序列的游程较大时,有利于敌方对该驻留频点的检测和干扰,降低了系统的抗干扰能力。实际工程中,可以将跳频序列进行宽间隔处理降低跳频序列的游程值。伪随机序列的游程特性有如下性质。

性质 1 长度为 s 游程出现数对序列的长度而言所占比例的数学期望为 $(q-1)^2/q^{s+1}$。

性质 2 总的游程出现数对序列保留的长度而言所占比例的数学期望为 $(q-1)/q$ [11]。

性质 3 长度为 s 游程出现数占总游程数比例的数学期望为 $(q-1)/q^s$。

从构造的长周期跳频序列中选取长度为 10^6 的局部序列进行游程特性测试,表 2 列出了局部序列游程特性的统计值和理论值的比较结果。由统计结果看出,不符合游程特性的测试标准,这与基于 L-G 模型构造跳频序列的生成方法有直接关系。

表 2　局部序列游程特性统计结果(1)

	出现数(理论值)	占总游程的比列(理论比例)
长度为 1 的游程	995872(992203 *)	99.836%(99.609% * * *)
长度为 2 的游程	1109(3876 *)	0.111%(0.389% * * *)
长度为 3 的游程	528(15 *)	0.053%(0.0015% * * *)
游程总数	997509(996094 * *)	100%

现对 L-G 模型进行改进,选用非连续抽头移位寄存器构造跳频序列,理论已证明可以改进跳频序列的游程特性。在相同条件下,再次进行游程特性测试,结果如表 3。可见,改进后的跳频序列与理论较符合,具有较好的游程特性,验证了游程特性统计方法的正确性。

表 3　局部序列游程特性统计结果(2)

	出现数(理论值)	占总游程的比列(理论比例)
长度为 1 的游程	996069(992203 *)	99.610%(99.609% * * *)
长度为 2 的游程	3894(3876 *)	0.389%(0.389% * * *)
长度为 3 的游程	6(15 *)	0.00006%(0.0015% * * *)
游程总数	999969(996094 * *)	100%

(注:* 根据性质 1,* * 根据性质 2,* * * 根据性质 3)

3　线性复杂度和抗预测性

3.1　线性复杂度

线性复杂度直接决定了跳频序列的抗破译能力。随机序列的线性复杂度定义为产生该序列的等效线性反馈移位寄存器(LFSR)的最小级数。对跳频序列测试时,一般采用二进制形式的跳频码序列进行 B-M 算法测试。

二进制序列的 B-M 算法:X 是长 L 的符合独立等概分布的二进制序列,线性复杂度的期望为:

$$E(C(X)) = \frac{L}{2} + \frac{1}{18}[4 + (L \bmod 2)] - 2^{-L}\left(\frac{L}{3} + \frac{2}{9}\right)$$

线性复杂度的期望基本为序列长度的一半,即 $L/2$。只要跳频序列的二进制表示形式的线性复杂度趋近于 $L/2$,则可以认为该序列具有理想的线性复杂度。跳频序列的复杂度充分大是必要的,但并不是越大越好,当跳频序列的复杂度接近序列长度时,在已知明文攻击下,可以由几个连续前项序列位确定后续的跳频序列,不能保证跳频序列的安全性[12]。

跳频序列的复杂度有很大差异, m 序列的线性复杂度较低,仅为移位寄存器级数 n;混沌序列、分组密码跳频序列、M 序列等均引入非线性运算,具有较理想的线性复杂度。

3.2　抗预测性

跳频序列的随机性和线性复杂度是跳频序列抗预测性能的重要方面,可以从密码学的视角更进一步研究跳频码的抗预测特性。跳频码序列的生成是以不同的地址码作为标示密钥(Key),对输入的实时时间(TOD)进行分组变换得到的[7]。根据分组密码学中抗密码破译的设计,需做如下要求:密文应对明文敏感,对密钥安全。将生成字长为 m 的跳频码序列看做密文,TOD 为明文,地址码为 Key,则定义描述变量如下:

(1)固定 Key,对连续输入的 TOD,相邻跳频码序列变动位数为 $k1$;

(2)固定 TOD,当 Key 某一位发生变动时,对应跳频码的变动位数为 $k2$。

可以要求:在上述两种情况下,随机变量 $k1$ 和 $k2$ 的数学期望为 $m/2$,其概率满足二项分布 $C_m^k\ (1/2)^m$。

在固定密钥 Key 时,对 256 频点长度为 10^6 的局部

跳频序列的抗预测性能进行测试,图 3 给出了 $k1$ 概率分布和二项分布的对比结果。可见,$k1$ 的概率分布基本符合二项分布,说明 m 序列对明文具有较好的敏感性。但 m 序列是移位寄存器的状态值与初始密钥通过模 2 加法运算得到的,使 m 序列对密钥 Key 的敏感性较差,当 Key 的某一位发生变动时,$k2$ 变动位数恒为 1,不能满足二项分布,说明 m 序列对密钥并不安全。综上,m 序列的抗预测性能较差,没有通过测试。

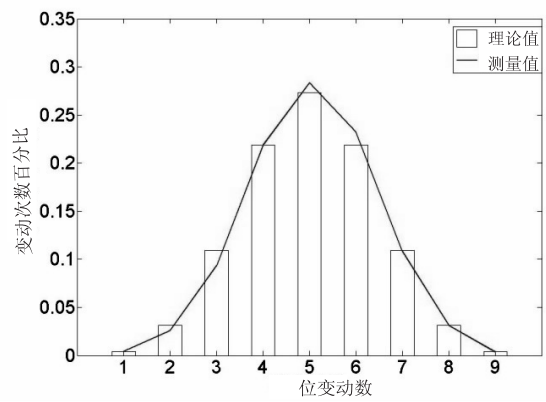

图 3 $k1$ 概率分布与二项分布对比结果

4 结束语

针对跳频通信的实际特点,重点分析局部跳频序列的各种特性,并以 m 序列为例分析讨论,给出了较为全面的局部序列性能评价指标,为跳频序列的设计和测试提供了更多参考。分析表明,截断后的 m 序列具有较好的平衡性、汉明相关性和频隙滞留特性,但游程特性不满足要求,在对 m 序列进行改进后游程特性得到较明显改善。跳频序列的抗破译性能不仅与序列的随机性和算法的复杂度有关,而且需要密码编码的角度考虑;分析表明m序列的随机性较好,但算法复杂度较低,对密钥不安全,可以得出 m 序列的抗破译性能较差的结论。

参考文献:

[1] 张申如,王庭昌,邓晓燕. 跳频码序列的统计监测[J]. 通信学报,1999,22(1):147-149.

[2] 易大进,李瑞欣,杨千里. 差分跳频图案性能检验探讨[J]. 铁道学报,2007,29(4):36-39.

[3] 李 赞,常义林,蔡觉平,等. 基于分组密码的跳频序列族构造[J]. 电子学报,2005(4):620-623.

[4] Chen Z, Li S, Dong B. A frequency transition function construction method of differential frequency hopping system [C]//60th IEEE Vehicular Technology Conference. Los Angeles:[s. n.],2004.

[5] Liu Z, Pan G, Wang T. Iterative Decoding of DFH System Based on SOVA[C]//The 4th International Conference on WiCOM. Dalian, China:[s. n.],2008:1-4.

[6] Nejad A Z, Aref M R. On the intelligent eavesdropping of differential frequency hopping[C]//Proc. of IEEE Wireless and Microwave Technology Conference. Clearwater, FL:[s. n.], 2006:1-5.

[7] 张申如. 跳频码序列动态特性和抗预测设计要求[J]. 应用科学学报,2004,22(1):102-106.

[8] 刘 方,彭代渊. 一类具有最优平均汉明相关特性的跳频序列族[J]. 电子与信息学报,2010,32(5):1258-1261.

[9] 李金涛,汪晓宁,王 祎,等. 基于 m 序列的宽间隔跳频序列的生成[J]. 电讯技术,2007,47(3):36-39.

[10] 周晓兰,张 杰. MATLAB 在通信系统中的应用[J]. 计算机技术与发展,2006,16(9):166-169.

[11] 张申如,梅文华,王庭昌,等. 非周期 q 元均匀随机序列的游程特性[J]. 通信学报,2000,21(1):45-48.

[12] 胡修林,胡晓娇. 跳频通信系统抗干扰性能仿真研究[J]. 计算机技术与发展,2007,17(2):39-42.

(上接第 168 页)

参考文献:

[1] 张 红,孙启美,李 峰. 基于蓝牙技术的手机与 PC 通信的实现[J]. 计算机时代,2007(6):62-63.

[2] 梁艳招,曾夏玲,段志锋,等. 基于蓝牙散射网的无线传感器网络研究[J]. 计算机技术与发展,2008,18(4):221-223.

[3] Denning D E. An Intrusion Detection Model[J]. IEEE Trans. on Software Engineering,1987,2(2):222-232.

[4] Debar H, Dacier M, Wespi A. Towards a Taxonomy of Intrusion Detection Systems[J]. Computer Networks, 1999, 31(8):805-822.

[5] Haartsen J. Bluetooth-The Universal Radio Interface for Ad Hoc Wireless Connectivity[J]. Ericsson Review, 1998(3): 110-117.

[6] 杨春光,余胜生. 蓝牙技术综述[J]. 当代通信,2003(21):46-49.

[7] 李启锐,刘灯宾,蔡湖锋,等. 蓝牙手机多媒体教学控制软件设计与实现[J]. 茂名学院学报,2010(3):43-46.

[8] 夏百战,何怀文,蔡凤菊. 一种基于蓝牙技术的多功能教学辅助系统[J]. 测控技术,2011,30(2):89-91.

[9] 马毅华,冯恩信. 基于 JSR-82 规范的 J2ME 蓝牙应用及其实现[J]. 无线电工程,2004,34(8):48-50.

[10] 俞国红. BlueIM:基于蓝牙的手机即时通信软件[J]. 计算机工程,2009,35(17):258-261.

[11] 陈雪林. 基于蓝牙的手机文件传输软件[J]. 计算机系统应用,2011,20(3):197-201.

[12] 杨 瑞. 基于蓝牙通信的短信平台设计与实现[J]. 计算机应用与软件,2011,28(2):218-219.

局部跳频序列特性分析

作者： 张世杰， 全厚德
作者单位： 军械工程学院,河北 石家庄 050003
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2012(9)