一种差分跳频码发生器的构造方法

董彬虹　　李少谦　　史锋旗
(电子科技大学通信抗干扰技术国家级重点实验室　成都　610054)

摘　要：针对差分跳频中常规 G 函数生成的跳频图案的 2 维连续性不够理想，其频率转移关系容易被窃听者截获的问题，该文提出了一种用 G 函数结合 PN 序列构成差分跳频码发生器的解决方法，对常规 G 函数和差分跳频码发生器产生的差分跳频图案的 2 维连续性进行了检验和比较，并对二者构成的差分跳频通信系统在 AWGN 条件下的误符号性能进行了理论分析，同时做出相应的计算机仿真，证实了采用 G 函数结合 PN 序列的差分跳频码发生器的设计方法在不损失系统误符号率性能的条件下，提高了系统的安全性。

关键词：差分跳频；G 函数；PN 序列；安全性
中图分类号：TN914.41　　**文献标识码**：A　　**文章编号**：1009-5896(2010)04-0816-05
DOI: 10.3724/SP.J.1146.2009.00456

A Differential Frequency Hopping Code Generator Construction Method

Dong Bin-hong　　Li Shao-qian　　Shi Feng-qi
(*National Key Laboratory of Communication, University of Electronic Science and Technology of China, Chengdu* 610054, *China*)

Abstract: An intelligent eavesdropper may easily intercept the frequency transition relations if a constant G function is used in Differential Frequency Hopping (DFH) system because of the poor 2-dimensional continuity of constant DFH sequence. To solve the problems, this paper puts forward a DFH code generator construction method which combines G function with PN sequence in a DFH system. The 2-Dimensional (2D) continuity performance of generated DFH patterns between constant G function and DFH code generator are tested and compared. The Symbol Error Rate (SER) performance in AWGN is analyzed in theory, and the corresponding simulation results are given. Theoretical analysis and simulation results show that the DFH code generator which combines G with PN sequence increases security of DFH system without decreasing the SER performance.

Key words: Differential Frequency Hopping(DFH); G function; PN sequence; Security

1　引言

近年，由于差分跳频技术有效地提高了短波通信的数据传输率，在跳频速率为 5000 跳/秒时，将短波通信速率提高到了 19.2 kps，因此受到越来越多的关注。差分跳频技术主要通过 G 函数将调制、编码和跳频技术相结合的方法提高在一定带宽下的数据传输率，实现跳频功能，因此 G 函数的设计应同时关注其对系统误符号性能影响和跳频图案的安全性。早期关于差分跳频技术的研究主要关注 G 函数的编译码方法及系统误码率性能分析[1−3]，而差分跳频技术作为一种新的短波扩频技术，其抗截获性能也开始受到关注。文献[4]指出，即使差分跳频序列的随机性很好，如果发射机采用固定 G 函数，由 G 函数决定的固定频率转移关系很容易被第 3 方截获，并按照截获的频率转移关系对合法的接收机发送不相关跳频序列进行干扰，降低合法接收机的抗干扰性能。文献[5，6]从安全性的角度出发，分别提出了一种优化的时变 G 函数的构造方法和基于高级加密标准(AES)的差分跳频 G 函数算法提高差分跳频图案的安全性，但并未对改进安全性的 G 函数算法是否影响系统的误符号性能进行分析。本文提出了一种 G 函数结合 PN 序列的差分跳频码发生器的构造方法，证明了其跳频图案的 2 维连续性达到了理想值，并与常规 G 函数产生跳频图案的 2 维连续性进行了检验和比较；给出了由差分跳频码发生器构造的差分跳频通信系统模型，并对其在 AWGN 条件下的误符号性能进行了理论分析，与采用常规固定 G 函数的系统误符号性能进行了计算机仿真比较，结果表明本文所采用的方法在不损失系统误符号率性能的条件下，提高了跳频图案的安全性。

2009-04-02 收到，2009-10-09 改回
国防重点实验室基金(9140C020103090C0201)资助课题
通信作者：董彬虹　bhdong@uestc.edu.cn

2　系统模型

2.1 常规的 G 函数模型

与常规跳频技术不同，差分跳频序列不是由伪码发生器控制，而是由上一跳的频率值 f_{n-1} 和当前跳的信息符号 X_n 共同来确定，可以用式(1)来表示[1]：

$$f_n = G(f_{n-1}, X_n) \tag{1}$$

其中的 G 函数是一种频率的编码函数，$f_n \in \{f_0, f_1, \cdots f_{M-1}\}$，$M$ 是跳频频率集的点数，可以用有向图的方式来直观地表达这种频率编码关系。图 1 中的每个节点代表频率集中的一个频点，每个节点分出 $f = 2^{\text{bph}}$ 个分支，bph 代表每跳所传输的比特数，每个分支上标注了当前的信息符号。以包含 $M = 8$ 频点的频率集为例，图 1 中共有 8 个节点，当每跳传输两个比特时，各节点有 4 个分支(00，01，10，11)。传输比特流按每 bph 个比特构成一个符号组成传输符号流，按照给定的差分跳频有向图产生相应的频率序列。

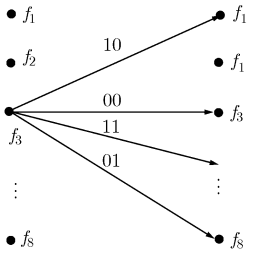


图 1 G 函数的有向图表示方法

当差分跳频通信系统发射机按照 G 函数决定的固有频率转移关系对数据信息序列进行调制，接收机采用最大似然接收规则解调接收信号时，误符号率性能取决于各合法频率转移路径的最小自由距离 ($d_{\min}$)，$d_{\min}$ 由 G 函数决定，是影响系统误符号率最主要的因素。按照文献[2]提出的构造方法和优化目标设计 G 函数，$d_{\min}$ 能够达到的最大理论值 $\lfloor \log M / \log f \rfloor$ ($\lfloor \bullet \rfloor$ 表示下取整)。可以用图 2 所示的“数→频”卷积编码模型表示文献[2]中的 G 函数构造方法[3,7]，其中编码器的初始状态为全 0，在跳频时钟的驱动下，每跳从移位寄存器的低位移入 bph 比特信息数据，同时从移位寄存器的高位移出 bph 比特数据后，移位寄存器的状态经过 2 进制到 M 进制转换后就是当前跳的输出频率 f_n，其中卷积码的约束长度为 $K = \log_2 M/\text{bph}$，码率为 $R_c = \text{bph}/\log_2 M$。

可以发现图 2 所示的 G 函数具有对称的结构，完全满足文献[2]提到的 G 函数的构造原则和优化目标，假定输入的信息数据序列为 01101100，输入的

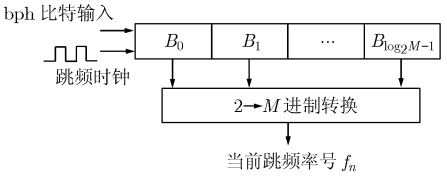


图 2 G 函数的“数→频”卷积编码模型

数据、移位寄存器的状态和输出的频率 f_n 的对应关系如表 1 所示。

表 1　$M = 64$，bph = 2 的 G 函数卷积编码

输入	移位	移位寄存器状态	f_n
	0	0 0 0 0 0 0	
10	1	1 0 0 0 0 0	f_1
01	2	0 1 1 0 0 0	f_6
11	3	1 1 0 1 1 0	f_{27}
00	4	0 0 1 1 0 1	f_{44}

2.2 改进后的差分跳频通信系统模型

改进后的差分跳频通信系统如图 3 所示，在发射机中加入了一个 PN 序列发生器对 G 函数产生的跳频序列加扰。

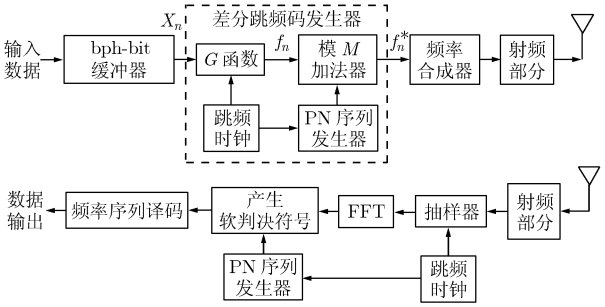


图 3 改进后的差分跳频通信系统

采用的加扰算法如下：

$$f_n^* = G(f_{n-1}, X_n, I_n) = f_{(n+I_n) \bmod M} \tag{2}$$

其中 I_n 是 PN 序列第 n 跳的输出，$0 \le I_n \le M-1$。G 函数与 PN 序列发生器共同构成差分跳频码发生器，为了在接收机的频率序列译码前恢复原始的差分跳频序列，需要在频率序列译码前增加与发射机结构相同且同步变化的 PN 序列。

3　差分跳频图案 2 维连续性分析

3.1 常规 G 函数生成跳频图案的二维连续性

理想的跳频图案的 2 维连续性要求各频率对出现的概率相等，即频率 f_{n-1} 出现后接着出现 f_n 的联合概率应相等

$$P(f_{n-1}, f_n) = 1/M^2, \quad f_n, f_{n-1} \in \{f_0, f_1, \cdots f_{M-1}\} \tag{3}$$

对于图 2 所示的 G 函数，当信源信息均匀分布，能够保证通信系统能够平均地使用各个频点，于是

$$P(f_{n-1}) = 1/M \tag{4}$$

由于前后跳频率存在固定的频率转移关系，2 维连续性为

$$P(f_{n-1},f_n)=\begin{cases}\dfrac{1}{fM}, & f_n\in G(f_{n-1},X_n)\\ 0, & \text{其他}\end{cases} \tag{5}$$

因此，如果差分跳频图案产生过程中频率转移关系不变，由于其 2 维连续性分布不均匀，很容易被第三方截获[4,5]。

3.2 差分跳频码发生器生成跳频图案的 2 维连续性

设计图 3 中 PN 序列的输出在 $[0,M-1]$ 随机均匀变化

$$P(I_n)=1/M,\quad 0\le I_n\le M-1 \tag{6}$$

于是，有

$$P(f_n^*\,|f_{n-1})=1/M,\quad f_n^*\in\{f_0,f_1,\cdots,f_{M-1}\} \tag{7}$$

由式(4)，式(7)和贝叶斯公式可得：

$$P(f_{n-1},f_n^*)=P(f_{n-1})P(f_n^*\,|f_{n-1})=1/M^2 \tag{8}$$

比较式(3)，式(5)和式(8)，可以看到，对 G 函数产生的跳频图案加扰后提高了差分跳频图案的 2 维连续均匀性，并达到了理想值。

对于差分跳频图案的 2 维连续性的检验，可以采用 χ^2 检验法[5,8]，设经过 L (L 充分大)次频率跳变，频率 f_i 出现后接着出现 f_j 的次数为 q_{ij}，计算统计量

$$\chi^2(M^2-1)=\sum_{i,j=0}^{M-1}\frac{(q_{ij}-L/M^2)^2}{L/M^2} \tag{9}$$

如果式(9)的计算结果 $\chi^2(M^2-1)$ 小于给定显著水平(例如 $\alpha=0.05$)下，自由度为 (M^2-1) 的理论值 $\chi^2_{0.05}(M^2-1)$ 时，则认为该跳频序列的各频率对满足均匀分布。

4 误符号性能分析

图 3 所示差分跳频通信系统可以等效为采用调制方式为 MFSK 的卷积码通信系统进行误符号率分析，如图 4 所示。其中的加扰器和解扰器，只是完成对跳频图案的加扰和解扰，并不影响系统的误符号率性能。因此对差分跳频通信系统误符号率的分析方法可以参照采用信道卷积编码时的差错概率的联合边界的推导方法[9]

设跳频时隙长度为 T，发送符号的基带等效表示为

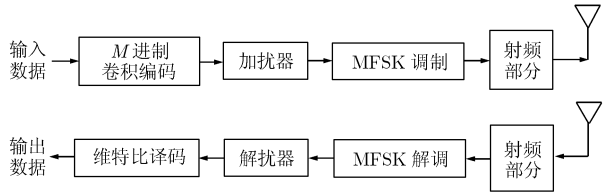


图 4 差分跳频的等效卷积码 MFSK 调制通信系统

$$s_m(t)=\mathrm{Re}[s_{lm}(t)e^{j2\pi f_c t}],\ m=1,2,\cdots,M,\ 0\le t\le T \tag{10}$$

式(10)中，$s_{lm}(t)$ 是等效低通信号，最佳相关型解调器产生 M 个复随机变量

$$r_m=r_{mc}+jr_{ms}=\int_0^T r_l(t)s_{lm}^*(t)\mathrm{d}t,\quad m=1,2,\cdots,M,\ 0\le t\le T \tag{11}$$

式(11)中，$r_l(t)$ 是等效低通接收信号，

$$r_l(t)=S_{lm}(t)e^{-j\phi}+n(t),\ m=1,2,\cdots,M,\ 0\le t\le T \tag{12}$$

式(12)中，ϕ 为随机相位，在 $[-\pi,\pi]$ 上均匀分布，$n(t)$ 为加性白高斯噪声，其单边功率谱密度为 N_0，如果采用软判决译码，则译码器的输入为

$$CM_m=\left|\int_0^T r_l(t)s_{lm}^*(t)\mathrm{d}t\right|^2 \tag{13}$$

首次差错事件概率的上边界为

$$P_e\le\sum_{d=d_{\mathrm{free}}}^{\infty}a_dP_2(d) \tag{14}$$

其中 a_d 表示与全零路径首次汇合且距离为 d 跳的路径的数目，$P_2(d)$ 为两条相差 d 跳的路径成对比较时的差错概率，$d_{\min}$ 为最小自由距离，当 $d_{\min}$ 达到最大值 $\lfloor\log M/\log f\rfloor$，错误路径与全零路径的距离大于或等于最小自由距离 $d_{\min}$ 时，每一次状态转移都有且仅有 $f-1$ 条路径与全零路径汇合，因此，式(14)可以表示为[10]

$$P_e\le\sum_{d=d_{\mathrm{free}}}^{\infty}(f-1)P_2(d) \tag{15}$$

文献[10]中对于 $P_2(d)$ 的推导比较复杂，$P_2(d)$ 可以认为是一个分集数为 d 的二进制正交信号在 AWGN 条件下的误符号率，因此[9]

$$P_2(d)=\frac{1}{2^{2d-1}}e^{-d\gamma/2}\sum_{n=0}^{d-1}C_n\left(\frac{1}{2}d\gamma\right)^n \tag{16}$$

式(16)中，$\gamma=E_s/N_0$，E_s 为发送信号的符号能量，定义

$$C_n=\frac{1}{n!}\sum_{k=0}^{d-1-n}\binom{2d-1}{k} \tag{17}$$

联合式(15)和式(16)，可以得到图 3 所示的差分跳频通信系统在 AWGN 条件下的误符号率上界为

$$P_e\le\sum_{d=d_{\mathrm{free}}}^{\infty}(f-1)\frac{1}{2^{2d-1}}e^{-d\gamma/2}\sum_{n=0}^{d-1}C_n\left(\frac{1}{2}d\gamma\right)^n \tag{18}$$

5 仿真及结果

通过通信链路仿真，可以进一步验证理论分析的正确性，便于对采用不同函 G 数的系统的跳频图案 2 维连续性和误符号率性能进行直观的比较。假设跳频频率集中的频率数 $M=64$，每跳携带比特数

bph = 2，PN 序列发生器采用 M 序列，帧长度为 $L = 1664$ 跳。

图 5 是分别采用常规 G 函数和差分跳频码发生器产生跳频图案的 χ^2 统计结果与 2 维连续性的理论值比较结果。(图例中：χ^2_{NG} 表示常规 G 函数，χ^2_{PNG} 表示差分跳频码发生器)：${\chi_T}^2$ 是显著水平 $\alpha = 0.05$ 下，自由度为 $M^2 - 1$ 的理论值，$\chi^2_T = 4244.7142$，这是可以接受检验结果为均匀分布的上限，当跳频图案的 2 维连续性 χ^2 统计结果小于理论值时，可以认为跳频图案中频率对的出现次数是均匀的。从图 5(a)中可以看出，χ^2_{NG} 远远大于 ${\chi_T}^2$，并且随着测试序列长度的增加这种趋势还在继续加大，从这个结果可以看到，常规 G 函数产生的跳频图案中频率对出现的次数不均匀，因此容易被第 3 方截获。

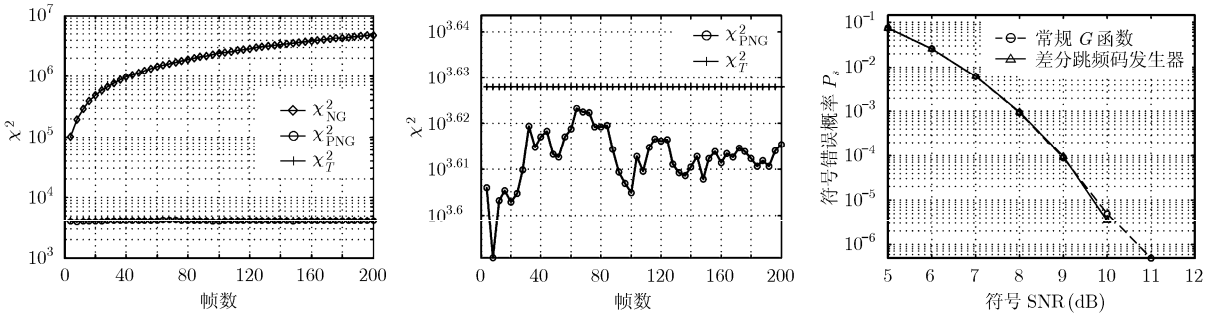
从图 5(a)的结果还可以看出，差分跳频码发生器产生的跳频图案的二维连续性 χ^2_{PNG} 远远小于 χ^2_{NG}，因此采用差分跳频码发生器相对于常规 G 函数提高了跳频图案的二维连续性，为了看清楚 χ^2_{PNG} 和 ${\chi_T}^2$ 的不同，将图 5(a)中的局部放大为图 5(b)，可以看到，χ^2_{PNG} 是小于 ${\chi_T}^2$ 的。因此，可以认为差分跳频码发生器产生的跳频图案中频率对出现的次数是均匀的，第 3 方很难截获其频率转移关系。

图 6 是在同等符号信噪比条件下对基于常规 G 函数的通信系统和基于差分跳频码发生器的通信系统符号差错概率的对比的仿真结果。

从图 6 的仿真结果可以看到，基于差分跳频码发生器的通信系统的误符号率与基于常规 G 函数的通信系统的误符号率基本上是相同的，因此可以得出基于 G 函数和 PN 序列的差分跳频码发生器设计方法在不损失系统误符号率的前提下，提高了系统的安全性。

6　结束语

由于常规 G 函数产生的跳频图案的 2 维连续性不够理想，其频率转移关系容易被第 3 方截获，因此不满足跳频通信系统的低截获率要求。采用 G 函数结合 PN 序列的差分跳频码发生器的设计方法，提高了差分跳频图案的 2 维连续性，在不损失系统误符号率性能的条件下提高了系统的安全性。



(a) 常规 G 函数、差分跳频码发生器跳频图案的 χ^2 统计结果比较

(b) 差分跳频码发生器跳频图案的 χ^2 统计结果与理论值比较

图 5 常规 G 函数、差分跳频码发生器的 χ^2 统计结果和理论值比较

图 6 常规 G 函数和差分跳频码发生器的误符号率的性能比较

参 考 文 献

[1] Herrick D L and Lee P K. CHESS: A new reliable high speed HF radio[C]. IEEE MILCOM'96, McLean Virginia, 1996: 684–690.

[2] Chen Z, Li S, and Dong B. A frequency transition function construction method of differential frequency hopping system, IEEE Vehicular Technology Conference 60th, Los Angeles, Sept 2004, Vol.7: 4692–4695.

[3] Liu Z, Pan G, and Wang T. Iterative Decoding of DFH System Based on SOVA, IEEE The 4th International Conference on WiCOM, Dalian, China, 2008: 1–4.

[4] Nejad A Z and Aref M R. On the intelligent eavesdropping of differential frequency hopping. Proc. IEEE Wireless and Microwave Technology Conference (WAMICON'06), Clearwater, FL, 2006: 1–5.

[5] Qu X, Wang S, and Li A. A method to improve 2D continuity performance of differential frequency hopping sequence. IEEE The 4th International Conference on WiCOM, Dalian, China, 2008: 12–14.

[6] 程莉, 周金荣. 基于高级加密标准(AES)的差分跳频 G 函数算法研究[J]. 舰船电子工程, 2008, 28(6): 107–120.
Cheng Li and Zhou Jin-rong. Differential frequency hopping G function algorithm based on advanced encryption standard[J]. *Ship Electronic Engineering*, 2008, 28(6): 107–120.

[7] 董彬虹, 李少谦, 陈智. 基于 TCM 的差分跳频 G 函数设计方法[J]. 电子科技大学学报, 2006, 35(4): 653–656.
Dong Bin-hong, Li Shao-qian, and Chen Zhi. TCM-based design method of G function for DFH system[J]. *Journal of University of Electronic Science and Technology of China*, 2006, 35(4): 653–656.

[8] 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): 121–124.
Yi Da-jin, Li Rui-xin, and Yang Qian-li. Performance test of differential frequency hopping patterns[J]. *Journal of the China Railway Society*, 2007, 29(4): 121–124.

[9] Proakis J G. Digital Communications. New York, McGraw-Hill, 2001: 351–353, 515–516.

[10] 陈智, 李少谦, 董彬虹. AWGN 下差分跳频通信系统的性能分析[J]. 信号处理, 2006, 22(6): 891–894.
Chen Zhi, Li Shao-qian, and Dong Bin-hong. Performance analysis of Differential Frequency Hopping System in AWGN[J]. *Signal Proccessing*, 2006, 22(6): 891–894.

董彬虹： 女，1972 年生，副研究员，研究方向为无线通信系统的抗干扰技术、差分跳频通信系统关键技术.

李少谦： 男，1957 年生，教授，博士生导师，研究方向为无线通信、移动通信中的关键技术.

史锋旗： 女，1980 年生，硕士，研究方向为差分跳频通信系统关键技术.