· 移动互联与通信技术 · 文章编号: 1000-3428(2018)02-0147-04 文献标志码: A 中图分类号: TP391

动态频谱抗干扰系统中动态宽间隔跳频序列研究

李胜男[1,2],李永贵[2],牛英滔[2],闫 岩[1],罗建翔[1]

(1. 解放军理工大学 通信工程学院,南京 210007; 2. 南京电讯技术研究所,南京 210007)

摘 要: 现有的跳频序列大多由于统计性能不佳,通信参数难以实时改变,无法直接应用于动态频谱抗干扰系统。为此,提出一种适用于动态频谱抗干扰系统的跳频序列。基于 m 序列,通过非连续抽头模型产生跳频基序列。依据随机平移替代法的思想,对基序列进行伪随机映射,给出一种频率数、跳频间隔可根据通信环境实时变化的动态宽间隔跳频序列构造方法。仿真结果表明,与基于固定参数的频率自适应跳频序列相比,动态宽间隔跳频序列在均匀性、随机性、汉明相关性、平均跳频间隔等方面均具有更好的性能。

关键词: 动态频谱抗干扰;跳频序列;m 序列;伪随机映射;跳频间隔

中文引用格式: 李胜男,李永贵,牛英滔,等. 动态频谱抗干扰系统中动态宽间隔跳频序列研究[J]. 计算机工程,2018,44(2):147-150,162.

英文引用格式: LI Shengnan, LI Yonggui, NIU Yingtao, et al. Research of Dynamic Wide-gap Frequency Hopping Sequences in Dynamic Spectrum Anti-jamming System[J]. Computer Engineering,2018,44(2):147-150,162.

Research of Dynamic Wide-gap Frequency Hopping Sequences in Dynamic Spectrum Anti-jamming System

LI Shengnan[1,2], LI Yonggui[2], NIU Yingtao[2], YAN Yan[1], LUO Jianxiang[1]

(1. College of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China;
2. Nanjing Telecommunication Technology Institute, Nanjing 210007, China)

【Abstract】 The existing Frequency Hopping (FH) sequence can not be directly applied to a dynamic spectrum anti-interference system due to poor statistical performance and difficulty in real-time changes of communication parameters. Therefore, a FH sequence suitable for dynamic spectrum anti-jamming system is proposed. Based on m sequence, a hopping base sequence is generated by discontinuous model. According to the idea of stochastic translational substitution, a pseudo-random mapping of base sequences is proposed, and a dynamic wide interval frequency hopping sequence congtruction method with frequency number and FH interval is qiven according to the changed communication environment. Simulation results show that the dynamic wide-gap hopping sequence has better performance in terms of uniformity, randomness, Hamming correlation, average hopping gap and so on, compared with the frequency-adaptive FH sequence based on fixed parameters.

【Key words】 dynamic spectrum anti-jamming; Frequency Hopping (FH) sequence; m sequence; pseudo-random mapping; frequency hopping gap

DOI: 10.3969/j.issn.1000-3428.2018.02.026

0 概述

作为跳频通信三大关键技术之一,跳频序列统计性能的好坏对跳频通信系统的抗干扰能力有着决定性的影响[1]。目前常用的跳频序列大多是针对频率数为素数的整数次幂(即 p^k,p 为素数)的跳频系统而设计的,而实际的跳频通信难以满足可用频率数为整数幂的要求[2]。为提高跳频系统的抗干扰能力,文献[3]在常规跳频系统的基础上提出了一种频率自适应跳频技术。它的主要思想是当系统检测或估计出干扰频率时,用无干扰或弱干扰频率替代干扰频率。但是,这种方法产生的跳频序列的均匀性和随机性等性能不佳。在动态频谱抗干扰系统[4-5]中,构成跳频频率表的频率数、频率值、分布带宽等频谱资源随着

基金项目:国家自然科学基金(61401505);江苏省自然科学基金。

作者简介:李胜男(1993—),女,硕士研究生,主研方向为无线通信、通信抗干扰技术;李永贵,高级工程师、硕士;牛英滔,高级工程师、博士;闫 岩、罗建翔,硕士研究生。

收稿日期:2017-01-13 修回日期:2017-02-20 **E-mail:** 18761685289@163.com

频谱感知的结果实时、动态变化,现有的跳频序列,由于参数难以实时改变、综合统计性能不佳,无法直接应用于动态频谱抗干扰系统中,因此,研究频率数、跳频间隔等通信参数可实时变化的跳频序列,是实现动态频谱抗干扰系统亟待解决的问题。

文献[6-7]基于重新映射思想,提出了一种频率数为 $p^k - p^m$ 的跳频序列产生方法,但其从根本上并没有跳出整数幂的思想。文献[8]基于分段映射、奇偶交替思想,提出了一种任意频率数跳频序列构造方法,该方法生成的序列具有较好的一维均匀性,但二维均匀性和随机性较差,同时频率数难以实时改变。文献[9]基于 3DES 算法,提出了一种任意频率数跳频序列构造方法,然而,3DES 算法属于公开算法,势必还会经历长期的攻击考验。

此外,对于跳速已经确定的系统来说,跳频序列设计成宽间隔跳频,能够有效分散干扰信号的出现时间,为纠错编码等措施的有效实施提供机会,从而进一步提高抗干扰能力[1]。目前产生宽间隔跳频序列最常见的思想是对跳频基序列重新进行宽间隔映射,主要方法有 2 种:一种是基于频带划分的思想,先将整个频带进行划分,使划分出的频带间满足宽间隔要求,再将跳频码根据一定的规则依次映射到相应频带上,如去中间频带法、对偶频带法[10-11]。这种方法以牺牲随机性和跳频增益为代价。另一种是基于频点修正的思想,以相邻或相关的跳频码为参考,对当前跳频码进行运算,使这些跳频码间满足宽间隔要求,如随机平移替代法、随机均匀转移替代法、双向预测法[12]。这种方法产生的跳频序列具有较好的跳频增益,但是均匀性大大降低[2]。文献[13-14]对随机平移替代法和随机均匀转移替代法的性能进行了比较,结果表明随机均匀转移替代法整体性能不如随机平移替代法。文献[15]针对随机平移替代法的平均跳频间隔较小、随机性差的问题,提出了一种改进的随机平移替代法,但其均匀性大大降低。

由于目前应用最广的跳频序列还是基于 m 序列构造的跳频序列,因此本文首先基于 m 序列,通过非连续抽头模型,产生跳频基序列。然后,根据频谱感知得出的可用频率数、跳频间隔等通信参数,基于随机平移替代法的思想,对跳频基序列重新进行伪随机映射,提出一种频率数、跳频间隔实时可变的动态宽间隔跳频序列构造方法。

1 系统模型

动态频谱抗干扰系统在传统无线通信系统中引入动态频谱接入思想,在对电磁环境实时、有效感知的基础上,通过智能决策及动态调整通信参数,提高无线通信系统的电磁环境适应能力,抗干扰能力和频谱利用率。如图 1 所示,假设系统中通信用户为 $U_k(k=1,2,\cdots,N_1)$,干扰用户为 $P_i(i=1,2,\cdots,N_2)$。假设每个通信周期分为 4 个阶段:同步阶段,频谱感知阶段,智能决策阶段和通信阶段。在时间同步阶段,系统中所有用户将本地的 TOD 调整为相同。实现 TOD 同步后,系统进入频谱感知阶段(这一阶段一直在进行,直到通信结束),所有通信用户对频谱环境进行感知,得到可用频谱集。在智能决策阶段,网控中心根据感知结果得到本周期内系统的通信参数(如频率数、跳频间隔、功率、调制方式等),以及系统所要实现的最优目标,对各通信用户的频谱分配和使用进行决策。在通信阶段,各通信用户根据决策结果进行通信。

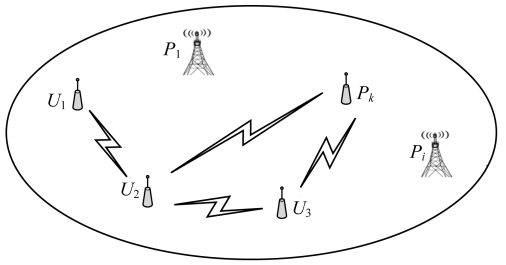

图 1 复杂电磁环境中的动态频谱抗干扰系统

为实现动态频谱抗干扰通信,必须设计一种能使信号在无干扰、可用信道上传输的动态宽间隔跳频序列。假设第 k 个周期内,无干扰、可用频率数为 q_k,跳频间隔为 D_k,则动态宽间隔跳频序列可表示为 $F=\{f_t \mid t=1,2,\cdots\}$,其中,$f_t \in \{1,2,\cdots,q_k\}$。

2 动态宽间隔跳频序列生成算法

基于上述假设,动态宽间隔跳频序列可以根据变化的通信参数实时生成。动态宽间隔跳频序列生成原理如图 2 所示。

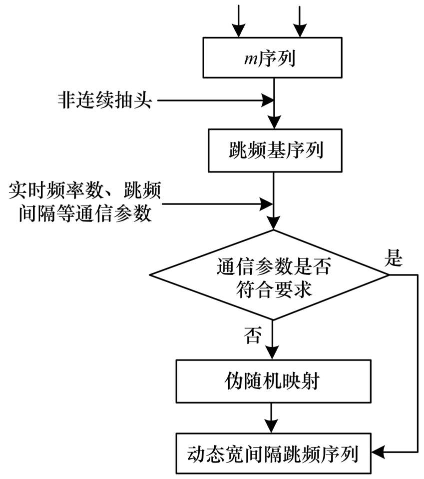

图 2 动态宽间隔跳频序列生成原理

2.1　跳频基序列的产生

首先利用 n 级本原多项式产生 m 序列。然后根据式(1)选取 r 个非相邻级抽头，产生独立伪随机跳频序列 S。其中，$S=\{s_t\}$，t 为时刻，$u=u_0u_1\cdots u_7$ 为地址码。

$$s_t=2^{r-1}\cdot[(a_t+u_0)\bmod 2]+\cdots+ 2\cdot[(a_{t+2(r-2)}+u_{r-1})\bmod 2]+ [(a_{t+2(r-1)}+u_r)\bmod 2] \tag{1}$$

2.2　伪随机映射

根据 k 周期内可用的频率数 q_k 和跳频间隔 D_k，由式(2)可得到 t 时刻的跳频码。通过时钟驱动，得到所需长度的跳频序列。

$$f_t=\begin{cases}s_t, s_t<q_k, d(f_{t-1},s_t)>D_k\\(s_t+D_k+1+shift_t)\bmod q_k,\text{其他}\end{cases} \tag{2}$$

其中，s_t 为跳频基序列 t 时刻对应的跳频码，f_t 为映射成宽间隔跳频序列 t 时刻对应的跳频码，$shift_t$ 为 $[0,q_k-2D_k-2]$ 上均匀分布的随机数，$d(f_{t-1},s_t)$ 为广义跳频间隔，$shift_t$ 和 $d(f_{t-1},s_t)$ 分别可由式(3)、式(4)表示。

$$shift_t=t\bmod[q_k-2D_k-1] \tag{3}$$

$$d(f_{t-1},s_t)=|f_{t-1}-s_t| \tag{4}$$

3　仿真性能与分析

为了验证本文提出方法产生的跳频序列的性能，本文从均匀性、随机性、汉明相关性、跳频间隔等方面对跳频序列进行性能分析，并与工程上应用广泛的基于固定参数的频率自适应跳频序列比较分析。仿真参数如表 1 所示。

表 1　仿真参数

参数	参数值
n	16
本原多项式的反馈抽头位置	[16,15,9,4]
u	$(01010101)_2$
r	8
α	0.5
q_k	96
D_k	10

3.1　均匀性

均匀性通常是指各跳频码出现的概率相等，即 $P(f_t=i)=1/q_k, i=1,2,\cdots,q_k$。序列的均匀性常用 χ^2 检验法验证。检验假设 $H_0=\{$序列服从均匀分布$\}$，则检验统计量为：

$$\chi^2=\sum_{f_t=1}^{q_k}\frac{[num(f_t)-L/q_k]^2}{L/q_k} \tag{5}$$

其中，$num(f_i)$ 表示在长度为 L 的序列中，跳频码 $f_t(f_t\in\{1,2,\cdots,q_k\})$ 出现的次数。在假设 H_0 下，若根据式(5)求得的 χ^2 值为 $\chi^2<\chi^2_{1-\alpha}(q_k-1)$，则在显著性水平 α 下接受 H_0。

在显著性水平 α 下，当 H_0 为真，且当 $L\to\infty$ 时，自由度为 q_k-1 的卡方检测理论参考值可由式(6)得到。

$$\chi^2_{1-\alpha}(q_k-1)=\frac{1}{2}(z_a+\sqrt{2(q_k-1)-1})^2 \tag{6}$$

其中，$z_a\approx 1.643$。

因此，当频率数为 96 时，自由度为 95，在显著性水平 $\alpha=0.5$ 的前提下，均匀性卡方检测的理论参考值 $\chi^2_{1-\alpha}(q_k-1)$ 为 118.4。

由图 3 可知，基于固定参数的频率自适应跳频序列的均匀性卡方检测值明显高于理论参考值，而动态宽间隔跳频序列的卡方检测值随着观察长度的增大而增大，总体略高于理论参考值。但是，动态宽间隔跳频序列明显具有更好的均匀性。

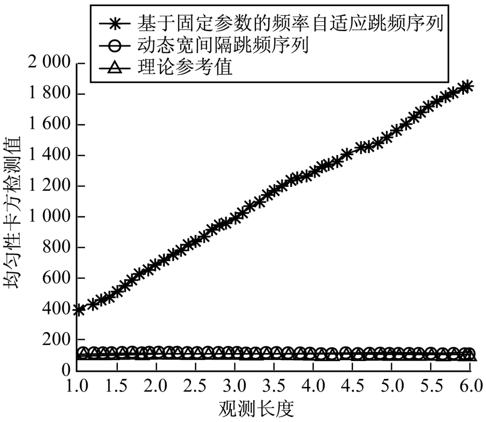

图 3　均匀性仿真曲线

3.2　随机性

随机性又称独立性，常用来表征 2 个随机数之间的统计相关性是否显著。序列的随机性常用列联表检验法检验。检验假设 $H_0=\{2$ 个序列相互独立$\}$，那假设长度为 L 的跳频序列为 $F_0=\{f_1,f_2,\cdots,f_L\}$，平移 τ 位后的序列为 $F_\tau=\{f_{1+\tau},f_{2+\tau},\cdots,f_{L+\tau}\}$。其中，$\tau=0,1,\cdots,L-1$。将两跳频序列中的跳频码按先后顺序两两分组，得到 $(f_1,f_{1+\tau})$，$(f_2,f_{2+\tau})$，$\cdots$，$(f_L,f_{L+\tau})$。记 n_{ij} 为各频率对出现的数量，$n_i=\sum_{j=1}^{q_k}n_{ij}$，$n_j=\sum_{i=1}^{q_k}n_{ij}$，则检验统计量为：

$$\hat{\eta}=n\left(\sum_{i=1}^{q_k}\sum_{j=1}^{q_k}\frac{n_{ij}^{\ 2}}{n_in_j}-1\right) \tag{7}$$

在假设 H_0 下，若根据式(7)求得的 $\hat{\eta}$ 值有 $\hat{\eta}<\chi^2_{1-\alpha}((q_k-1)^2)$，则在显著性水平 α 下接受 H_0。当频率数为 96 时，自由度 $(q_k-1)^2=95^2$，在显著性水平 $\alpha=0.5$ 的前提下，随机性卡方检测的理论参考值 $\chi^2_{1-\alpha}((q_k-1)^2)$ 为 9 246.6。

由图 4 可知，在码子距离小于 10 时，基于固定

参数的频率自适应跳频序列的随机性卡方检测值高于理论参考值，而动态宽间隔跳频序列的卡方检测值始终低于理论参考值。因此，动态宽间隔跳频序列具有较好的随机性。

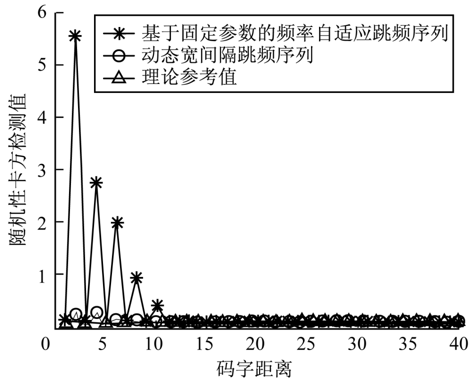

图 4 随机性仿真曲线

3.3 汉明相关性

汉明相关性分为汉明自相关和汉明互相关，它们表征了序列间的碰撞特性，反映了系统的抗衰落能力和用户间组网的碰撞情况。周期为 L 的 2 个序列在时延 $H_{F_0F_1}(\tau)=\sum_{j=1}^{L}h[f_1(j),f_2(j+\tau)]$ 时的周期汉明相关定义为：

$$H_{F_0F_1}(\tau)=\sum_{j=1}^{L}h[f_1(j),f_2(j+\tau)] \tag{8}$$

其中，$f_1(j),f_2(j+\tau)\in\{1,2,\cdots,q_k\}$，$j+\tau$ 以模 L 运算，且：

$$h[f_1(j),f_2(j+\tau)]=\begin{cases}0,f_1(j)\neq f_2(j+\tau)\\1,f_1(j)=f_2(j+\tau)\end{cases} \tag{9}$$

由定义可知，汉明相关值越小，汉明相关性越好。

由图 5、图 6 可知，动态宽间隔跳频序列的汉明自相关值和汉明互相关值，都略低于基于固定参数的频率自适应跳频序列的汉明自相关值和汉明互相关值。因此，可以认为动态宽间隔跳频序列具有更好的汉明相关性。

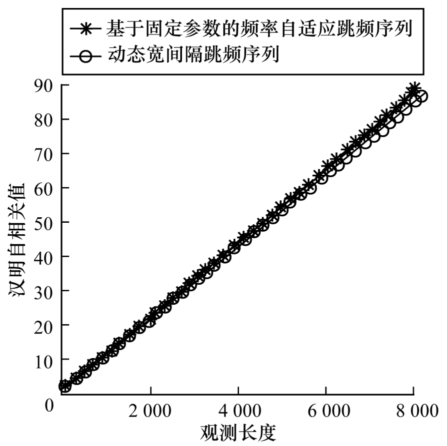

图 5 汉明自相关性仿真曲线

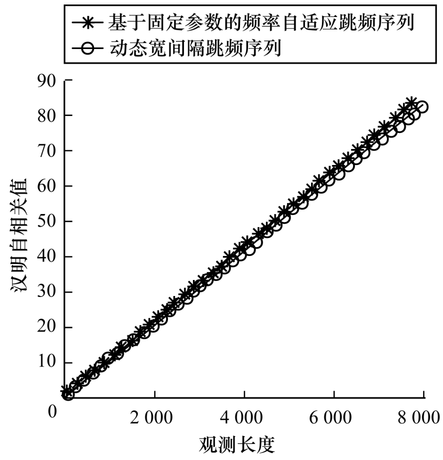

图 6 汉明互相关性仿真曲线

3.4 跳频间隔

跳频间隔一般由平均跳频间隔来检验。平均跳频间隔是指任意连续两跳的跳频码之差的绝对值的平均值。

由图 7 可知，动态宽间隔跳频序列的平均跳频间隔明显高于基于固定参数的频率自适应跳频序列的平均跳频间隔。因此，可以认为动态宽间隔跳频序列的跳频间隔特性更好。

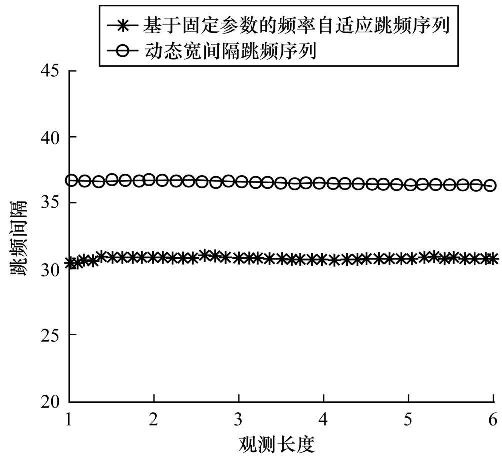

图 7 跳频间隔仿真曲线

4 结束语

动态频谱抗干扰系统中的跳频序列需要具备实时性、统计性能等特点，而现有的跳频序列难以满足上述要求。为此，本文基于 m 序列，利用随机平移法，提出一种通信参数可根据频谱环境实时变化的跳频序列构造方法。仿真结果表明，与基于固定参数的频率自适应跳频序列相比，本文提出的跳频序列具有较好的均匀性、随机性、汉明相关性及较大的跳频间隔。

（下转第 162 页）

4 结束语

以分组密码 AES 为核心设计的流密码算法 LEX 是现代流密码算法设计的一种重要方法。但 LEX 算法的结构缺陷,引发了众多密码界学者对其进行分析和攻击,其中又以滑动攻击最为有效,只需要 2^{61} 个初始输入 $\boldsymbol{IV}$ 和 2×10^{4} Byte 的密钥流,就可以完全恢复出 128 bit 密钥[15]。本文以 LEX 算法为基础,对其密钥体系进行改进,使其每组 AES 的加密密钥均不同,具备抵抗滑动攻击的能力,提高了 LEX 算法的安全性,并且保持了 LEX 算法较高的运行速度。同时,实验仿真结果表明,改进后的算法延续了 LEX 算法良好的随机特性。由于算法本身的结构与运算并未做调整,因此改进后的算法在其他方面性能与 LEX 算法相当。

参考文献

[1] ECRYPT. eSTREAM:ECRYPT Stream Cipher Project, IST-2002-507932 [EB/OL]. (2004-02-11). http://www.ecrypt.eu.org/stream.

[2] HASTAD J, NASLUND M. The Stream Cipher Polar Bear[EB/OL]. (2005-02-10). http://www.ecrypt.eu.org /strearm/.

[3] BIRYUKOV A. A New 128-bit Key Stream Cipher LEX[EB/OL]. (2005-06-13). http://www.ecrypt.eu.org/stream/ciphers/lex/lex.pdf.

[4] National Institute of Standards and Technology. Announcing the Advanced Encryption Standard(AES)[EB/OL]. (2001-11-26). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[5] HENRICKSEN M. Flexible Block Ciphers: Modifying LEX[C]//Proceedings of IEEE International Conference on Computer Science & Information Technology. Washington D. C., USA: IEEE Press, 2010: 630-634.

[6] VELICHKOV V, RIJMEN V, PRENEEL B. Algebraic Cryptanalysis of a Small-scale Version of Stream Cipher LEX[J]. Information Security, 2010, 4(2): 49-61.

[7] 张中亚,关 杰. 对流密码算法 LEX 的差分故障攻击[J]. 上海交通大学学报(自然科学版),2012,46(6):865-869.

[8] WU Hongjun, PRENEEL B. Attacking the IV Setup of Stream Cipher LEX[EB/OL]. (2006-03-15). http://www.ecrypt.eu.org/stream/papersdir/059.pdf.

[9] 邓元庆,龚 晶,石 会. 密码学简明教程[M]. 北京:清华大学出版社,2011.

[10] 李佳雨,石 会,邓元庆,等. 抗滑动攻击的 LEX 算法改进及分析[J]. 通信技术,2015,48(2):203-207.

[11] 李 欣,谭晓青. 抵抗滑动攻击的 LEX 算法改进[J]. 计算机工程与应用,2012,48(26):101-103.

[12] 尤加勇,李 超. 针对 LEX 算法的截断滑动攻击[J]. 信息安全与通信保密,2007(9):96-98.

[13] 国家秘密管理局. 随机性检测检测规范:GM/T0005-2012[M]. 北京:中国标准出版社,2012.

[14] 李佳雨,石 会,邓元庆,等. 针对流密码 LEX 的差分故障攻击及算法改进分析[J]. 计算机科学,2015,42(11):352-356.

[15] 李佳雨. 流密码算法 DLEX 设计与分析[D]. 南京:解放军理工大学,2015.

编辑 顾逸斐

(上接第 150 页)

参考文献

[1] 梅文华. 跳频序列设计[M]. 北京:国防工业出版社,2016.

[2] 关 磊. 高性能智能跳频序列族构建与组网理论研究[D]. 西安:西安电子科技大学,2015.

[3] 姚富强. 通信抗干扰工程与实践[M]. 2 版. 北京:电子工业出版社,2012.

[4] 朱毅超,陆建勋. 动态频谱抗干扰系统在部分频带干扰下的性能[J]. 电子学报,2011,39(10):2331-2337.

[5] 朱毅超,梁 亮,田 骅,等. 一种基于认知的动态频谱抗干扰新技术[J]. 通信技术,2014,47(1):71-75.

[6] PARK S B, LEE K E, CHOI Y K, et al. Some Good Frequency Hopping Sequences with Arbitrary Number of Slots [C]//Proceedings of IEEE MILCOM'01. Washington D. C., USA: IEEE Press, 2001: 1325-1329.

[7] 李 赞,廖丽思,金力军,等. 适用于任意频隙数的跳频序列族产生方法研究[J]. 无线电工程,2004,34(4):1-3.

[8] 耿阿囡,黄训诚,庄奕琪,等. 一种任意频隙跳频序列构造方法[J]. 通信技术,2007(4):54-56.

[9] GUAN L, LI Z, XIAO S, et al. A Family of Adaptive Frequency Slot Number FH Sequences for High Security and Reliability Communication [C]//Proceedings of EISIC'15. Washington D. C., USA: IEEE Press, 2015: 30-36.

[10] 韩 明,赵洪林. 采用分割频带法构造宽间隔跳频序列[J]. 电讯技术,2014,54(11):1516-1521.

[11] 罗 翔,周三文,焦东立,等. 一种基于 RS 码的宽间隔跳频序列生成方法[J]. 遥测遥控,2015(1):24-29.

[12] GUANG L, LI Z, SI J, et al. Generation and Characteristics Analysis of Cognitive-based High-performance Wide-gap FH Sequences [J]. IEEE Transactions on Vehicular Technology, 2015, 64(11): 5056-5069.

[13] 何维苗. 一种新的实现宽间隔跳频的方法——随机平移替代法[J]. 现代军事通信,1999,7(4):13-15.

[14] 何维苗,冯 冈. 构造宽间隔跳频码序列的两种算法之比较[J]. 解放军理工大学学报(自然科学版),2004,5(4):29-33.

[15] 冯建利,赵裔昌. 一类改进的随机平移替代法构造的宽间隔跳频序列[J]. 电讯技术,2013,53(9):1175-1192.

编辑 索书志