相关跳频通信系统安全性分析

李天昀，胡宗云，葛临东

(郑州信息工程大学信息工程学院 郑州 450002)

【摘要】分析了相关跳频通信系统中频率序列的检测以及纠错译码，并从第三方接收的角度探讨了相关跳频信号的接收、译码以及转移函数反推的复杂度。分析结果表明：相关跳频通信并不是一种抗截获的无线通信方式，其通信安全是建立在转移函数机制上的。转移函数反推的复杂度非常高，给相关跳频通信体制提供了很好的安全性。

关 键 词 相关跳频; 转移函数; 最大似然译码; 通信安全
中图分类号 TN97 文献标识码 A

Security Analysis of DFH Communication System

LI Tian-yun，HU Zong-yun，GE Lin-dong

(School of Information Engineering, University of Information Engineering Zhengzhou 450002)

Abstract The frequency sequence detection and error-correcting decoding are analyzed in Differential Frequency Hopping (DFH) communication system. From the viewpoint of the third party of communications, the receiving and decoding process and the complexity of transition function analysis are discussed. The results show that DFH is not a LPI communication manner, and its security relies on the transition function. The complexity of transition function analysis is very high, which provides very high security to DFH communication system.

Key words differential frequency hopping; transition function; maximum likelihood decoding; communication security

1 相关跳频及频率转移函数简介

相关跳频通信技术是美国1995年推出相关跳频电台(Correlated Hopping Enhanced Spread Spectrum，CHESS)时首次提出的一种无线数据传输方式[1-2]，是一种新的高速抗干扰宽带跳频通信体制。相关跳频也叫差分跳频(Differential Frequency Hopping，DFH)，采用频率转移函数机制来控制频率跳变序列并传输信息。频率转移函数G定义为：$F_n=G(F_{n-1}, X_n)$，其中X_n为当前传输的数据符号；F_{n-1}为前一跳频率值；F_n为当前跳变频率，传输的数据信息被调制到跳变频率序列相邻频点的变化中。设每跳中X_n携带的信息为B_h bit，跳变频率集为：$S=\{f_1, f_2, \cdots, f_N\}$。通常$N$取2的整数幂，且$N>2^{B_h}$，如CHESS系统中$N$取64或256，$B_h$取1、2或4。在发射端，原始数据先按$B_h$ bit分组，由当前传输的B_h bit和F_{n-1}来决定F_n，每跳传输的都是单频脉冲。接收端检测到跳变频率序列后仅需根据频率转移关系和频点间的相关性来进行纠错和译码，从而可以使跳频系统获得更高的跳速，并减小对其他共享带宽用户的干扰，实现可靠的高速数据传输。

$$\boldsymbol{T}_o=\begin{array}{c|cc} & 0 & 1 \\ 1 & 1 & 2 \\ 2 & 3 & 4 \\ 3 & 5 & 6 \\ 4 & 7 & 8 \\ 5 & 2 & 1 \\ 6 & 4 & 3 \\ 7 & 6 & 5 \\ 8 & 8 & 7 \end{array} \qquad \boldsymbol{T}_i=\begin{array}{cc|c} 0 & 1 & \\ \hline 1 & 5 & 1 \\ 5 & 1 & 2 \\ 2 & 6 & 3 \\ 6 & 2 & 4 \\ 3 & 7 & 5 \\ 7 & 3 & 6 \\ 4 & 8 & 7 \\ 8 & 4 & 8 \end{array}$$

a. 出阵 b. 入阵

图1 频率转移矩阵

频率转移函数可以描述成频率转移矩阵、状态图、树图等直观模型。频率转移矩阵是N行2^{B_h}列的矩阵，可以表示成出阵和入阵两种不同形式。在出阵$\boldsymbol{T}_o$中，元素$\boldsymbol{T}_o(i, j)$表示从频率编号为：i, $i=1,2,\cdots, N$的频点f_i出发，当输入信息为：j, $j=0, 1,\cdots, 2^{B_h}-1$时，将转移到编号为$\boldsymbol{T}_o(i, j)$的频率，而在入阵$\boldsymbol{T}_i$中，$\boldsymbol{T}_i(i, j)$表示输入信息为j时，转移到频点i，需要从频点$\boldsymbol{T}_i(i, j)$出发。图1所示给出了$N=8$，$B_h=1$时的一个频率转移矩阵，其中频点f_i简记为其编号i。

收稿日期：2004 – 04 – 05
作者简介：李天昀(1979 –)，男，博士生，主要从事通信信号处理及软件无线电方面的研究.

2 相关跳频信号的接收和译码

2.1 频率序列检测

在CHESS系统中对采样数据进行信号检测由数字接收单元完成[1-2]，采样数据分为I、Q两路后进行频域分析，根据幅度谱来检测跳变频率。另外，在一些文献中也提到一些别的检测算法，如采用非相干检测的解跳结构[3]、基于STFT的跳检测方法等[4]。

2.2 最大似然译码

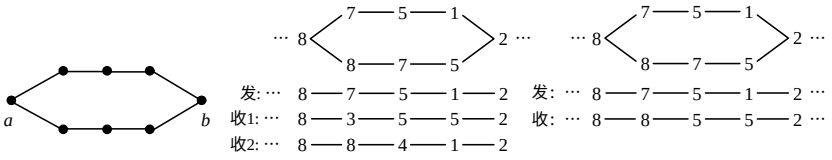
相关跳频序列的译码根据频点间的相关性来纠错。定义距离d为所有始点和终点的频率都相同的两条互异的等长频率转移路径之间的汉明距离，转移函数的设计如果使频点转移路径满足最小距离最大，则可获得最大的相关纠错能力。适当设计转移函数G，可使最小距离达到如下最大值：

$$\sigma = \max_{G}(\min(d)) = \left\lfloor \frac{\log_2 N}{B_h} \right\rfloor \tag{1}$$

此时最大可以纠连续的$\sigma-1$个错。一般N、B_h的取值满足$\log_2 N$为B_h的整数倍，此时$\sigma=\log_2 N / B_h$。

译码过程根据转移函数来进行。频率转移过程可以表示成格图(Trellis)或树图(Tree)的形式，是一个有限状态机，可采用最大似然译码方法来进行译码。下面从几种特殊错误模式的分析出发，分析最大似然译码的纠错性能以及相关跳频参数对纠错性能的影响。

以图1所示的转移函数为例，N=8，B_h=1，min(d)=σ=3，即满足最小距离最大。对随机的一个错误可纠，且最大只可纠连续的2个错误，而对于连续的3个错误一般是不可纠的。对于连续2个频率检测错误的情况，有的错误模式也是不可纠的。如图2a所示，从a点经过4步转移到b点总存在两条路径。如果发的是第一条路径，而检测频点时错了两个频点而且其中一个正好错到另一条路径上，则这种错误不可纠，如图2b所示。而如果两个频点都正好错到另一条路径上，则会出现认为可纠但是纠得不对的情况，如图2c所示。这两种情况一旦译错，都将是连续的三个频点译码错误。同样，对于从a点经过5步转移到b点的4条路径，也可以分析其有两个频点检测错误时的特殊错误模式。



a. 转移路径　　b. 错误模式　　c. 错误模式

图2　最大似然译码特殊错误模式

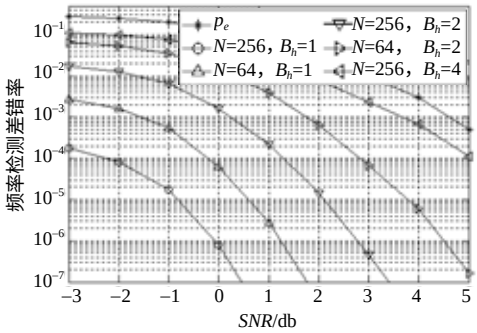


图3　最大似然译码频率检测差错性能

对类似图2b所示的不可纠的错误，在译码过程中将产生多条具有相同的最小距离度量的最大似然路径。设有M条最大似然路径，任选其中一条作为发送路径，则正确译码的可能性为$1/M$。

假设转移函数符合最大相关纠错性能，如果接收频率序列中每个频点出错的概率为p_e，忽略出现概率相对较小的特殊错误模式，则译码后频率序列的符号错误概率p_d约为：

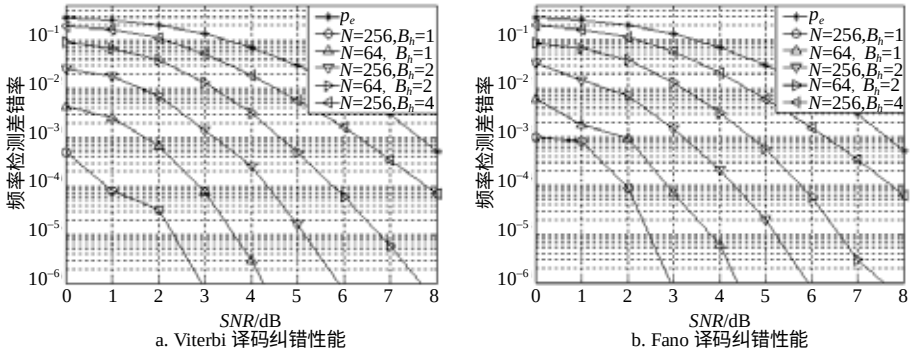
$$p_d \approx C_{\sigma}^{\sigma-1}(1-p_e)^3 p_e^{\sigma-1} \frac{C_{\sigma-1}^{1}(2^{B_h}-1)(N-1)^{\sigma-2}}{(N-1)^{\sigma-1}} \sigma \frac{2^{B_h}-1}{2^{B_h}} +$$

$$(1-p_e)^2 p_e^{\sigma} \sigma \frac{2^{B_h}-1}{2^{B_h}} + C_{\sigma-1}^{1}(1-p_e)^3 p_e^{\sigma} \frac{[2(2^{B_h}-1)+(\sigma-2)((2^{B_h})^2-1)](N-1)^{\sigma-1}}{(N-1)^{\sigma}} (\sigma+1) \frac{(2^{B_h})^2-1}{(2^{B_h})^2} \tag{2}$$

式中　第1项为类似于图2b所示连续σ个频点检错$\sigma-1$个时的特殊错误模式；第2项为连续检错σ个频点的情况；第3项为除第2项的情形外在连续$\sigma+1$个频点范围内出现σ个频率检测错误时的特殊错误模式；其余错误

模式被忽略。由上式得到理论上的检测性能如图3所示。

实际译码过程可以采用Viterbi算法或Fano算法，Viterbi译码是最优译码，Fano译码的纠错性能接近于Viterbi译码。译码纠错性能的仿真结果如图4所示，可见这两种译码方法的性能与图3所示的分析结果基本一致。



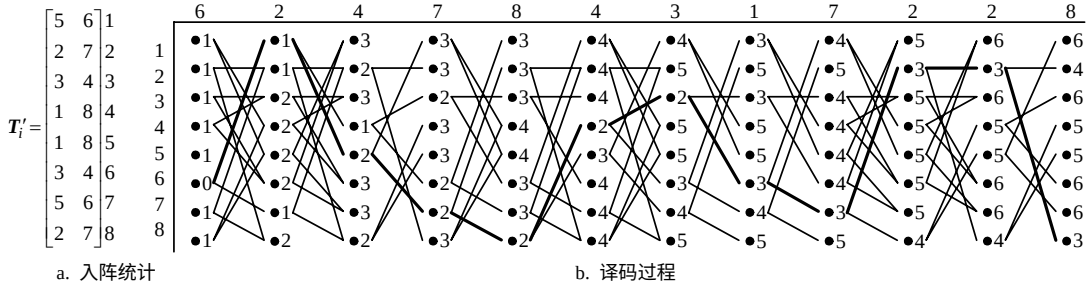
a. Viterbi 译码纠错性能　　b. Fano 译码纠错性能

图4　频率检测差错性能仿真结果

3　相关跳频通信的安全性分析

3.1　第三方的接收和译码

对于第三方的接收，通过类似CHESS系统的频率检测方案，亦可在频域进行频率检测。在检测得到频率序列后，可以对其通过统计来准确地估计出跳变频率集，从而得出估计的跳变频率序列。从上述估计的跳变频率序列中，统计相邻频点之间的转移关系，抛弃出现概率相对较小的转移关系，可分析出参数B_h以及频率转移矩阵，只是频率的转移所对应传输的信息是未知的。由频率转移关系已经可得出频率转移的网格图，根据此网格图可以通过Viterbi译码算法或序列译码算法来进行纠错译码，得出频率差错概率相当低的跳变频点序列。



a. 入阵统计　　b. 译码过程

图5　Viterbi译码过程图示

假设通信中采用如图1所示的转移函数，第三方对检测的频率序列进行分析得出频点数为N=8，B_h=1，并得出跳变频率集S。对跳变频率集中的频点进行编号(第三方的频率编号与图1所示的编号不一致)，从估计的跳变频率序列中统计得出的对应信息不确定的频率转移矩阵(入阵) $\boldsymbol{T}_i'$ 如图5a。设频点序列的前面一段为“6,2,4,7,8,4,3,1,7,2,2,8”，则采用汉明距离作为距离度量来进行Viterbi硬判决译码的译码过程如图5b所示。其中，格图上方列出的是接收频率序列，图左为格图中节点的频率编号，格图中节点旁列出的数字为从起点到该节点的幸存路径的距离度量。在译码过程中不需要初始同步，这有利于第三方的译码。图中加粗的路径为回溯的路径，由此译出纠错后的频率序列“6,1,5,7,8,4,3,6,7,2,2,8”，纠正了三个频点检测错误。

由图3中的最大似然纠错译码差错概率性能可知，译码后的频率序列差错概率将相当小。此时，虽然第三方已经得到了可信度非常高的跳变频率序列，但是还不能译出所携带的信息，因为转移函数对于第三方来说是未知的。

由以上分析可知，相关跳频通信并不是一种抗截获的无线通信方式，信号接收中的宽带采样及频率检测方式，对于通信方的接收机和第三方的接收机来说，其条件是一样的。第三方完全可以采用频域分析的

方法检测到跳变频率序列，统计出转移概率矩阵，并进行纠错译码。而频率转移函数对于第三方来说是未知的，第三方在接收译码后并不能译出所携带的信息。因此，相关跳频通信的通信安全是建立在转移函数机制上的。

3.2 转移函数的安全性

频率转移函数是相关跳频通信技术中的关键技术，决定整个通信系统的性能。一般，转移函数的设计中需要考虑其相关纠错性能以及频点使用的均匀性和随机性等。均匀性和随机性要求转移函数满足各频点的出度和入度均相同，且如果将频率集S看成Markov链的状态集，则要求S对于状态转移过程是不可约的。现有的一些转移函数设计方法包括基于线性空间坐标变换的设计方法[6]、分组编码方法等[7]。

假设对应信息未知的频率转移矩阵$\boldsymbol{T}'$已知，并且没有其他可资利用的先验知识，下面分析第三方根据$\boldsymbol{T}'$以及译码后的跳变频率序列来反推各状态转移与传输数据符号之间对应关系时的复杂度。

$\boldsymbol{T}'$为$N \times 2^{B_h}$的矩阵，其中每行的元素是确定的，即从某频点出发可能转移到的2^{B_h}个频点已统计得出。但是各元素所携带的信息不确定，即每行中元素的排列次序不能确定。如果采用穷举的方法来反推转移函数，显然，需穷举的转移函数个数为$C=((2^{B_h})!)^N$。在N=64、B_h=2时约为$C=2^{293}$。可见，其穷举复杂度是非常高的，并且，N、B_h的值越大，其穷举的复杂度也越大。

实际应用的频率转移函数一般满足使频率转移矩阵$\boldsymbol{T}$中的每一列为所有频点的一个全排列。如果考虑这点，则由$\boldsymbol{T}'$反推$\boldsymbol{T}$的穷举复杂度有所下降。例如采用分组编码方案设计的N=64、B_h=2时的转移函数，由$\boldsymbol{T}'$反推$\boldsymbol{T}$且考虑$\boldsymbol{T}$中每列都是所有频点的一个全排列时，需穷举的转移函数个数为$(4!\times 9\times 4)^{16}$，即穷举复杂度约为$C=2^{156}$，相当于是156位密钥的穷举破译，其保密程度是很高的。

在转移函数穷举反推过程中，还有一个问题是对穷举出的每个转移函数的判决标准。如果在转移函数反推过程中进一步考虑转移函数的最大相关纠错性能等设计准则，则在穷举过程中可以根据设计准则剔除部分穷举出的转移函数。而对剩余的穷举出的转移函数要判断其是否是发射机所采用的转移函数，需要通过该转移函数对跳变频率序列进行试译码，译出所携带信息，并根据信息的合理性来判断。而这个过程是非常费时的，而且信息合理性的自动判决标准也不好选择。

可见，侦收方虽然可以截获相关跳频信号，但是在对转移函数进行破译分析时的复杂度是非常大的，转移函数机制给相关跳频通信方式提供了很好的安全性。

4 结 论

对相关跳频通信系统中频率序列检测方案以及纠错译码过程进行了深入分析，并从第三方接收的角度探讨了相关跳频信号的接收、译码以及转移函数反推的复杂度，论证了相关跳频通信的安全性。通信的第三方完全可以采用频域检测的方法来检测频率序列，并统计分析出跳变频率集以及转移关系，从而进行纠错译码，得出差错概率非常低的跳变频率序列。因此，相关跳频通信并不是一种抗截获的无线通信方式。相关跳频通信系统的通信安全是建立在转移函数机制上的。转移函数反推的穷举复杂度分析表明，转移函数机制给相关跳频通信体制提供了良好的安全性。相关跳频通信体制不仅提供了短波高速数据传输问题的一种解决途径，而且还是一种保密性能非常好的通信方式。

参 考 文 献

[1] Herrick D L, Leep K. CHESS: a new reliable high speed HF radio[C]// MILCOM'96, Washington,DC: 1996: 684-690.
[2] Herrick K D L, Lee P K. Correlated frequency hopping: an improved aproach to HF spread spectrum communications[C]// Proceedings of the 1996 Tactical Communications Conference, Fort Wayne, USA: 1996: 319-324.
[3] 董彬虹, 李少谦, 陈 智, 等. 差分跳频信号最佳接收机设计[J]. 电子科技大学学报, 2003, 32(5): 530-534.
[4] 刘忠英, 张 毅, 姚富强. 基于STFT与G函数相结合的短波DFH跳检测方法[J]. 电子学报, 2003, 31(1): 13-16.
[5] Proakis G. Digital communications(4e)[M]. Columbus: The McGraw-Hill Companies Inc., 2001.
[6] 陈 智, 李少谦, 董彬虹, 等. 一种差分跳频系统的频率转移函数[J]. 电子科技大学学报, 2003, 32(5): 525-529.
[7] 李 明, 戚仁华, 朱红琛. 短波宽带快速跳频通信技术研究[J]. 通信技术, 2000, 110 (3): 34-37.

编 辑 孙晓丹