

# 基于 DMR 标准的信道编解码研究

刘二晓, 李玉柏, 李 桓

(电子科技大学 DSP 教研室, 成都 611731)

**摘要:** 为了提高 DMR 系统基带算法的性能, 分析研究了 DMR 标准中的 3/4 率网格码和二次剩余码。针对 3/4 率网格码, 提出两种译码算法, 方法 1 充分利用了有限状态机的特性, 方法 2 将维特比译码算法中的蝶形运算进行推广改进。针对 QR 码, 通过计算校验多项式的码重进行译码。MATLAB 下的仿真结果表明, 3/4 率网格码的两种译码方法性能相差不大, 但方法一的计算量少, 易于工程实现。QR 码的译码算法不仅有效地避免了计算复杂的错误位置多项式, 而且提高了相同信噪比下的译码性能。

**关键词:** DMR 系统; 3/4 率网格码; 维特比译码; 二次剩余码; 伴随多项式的码重

**中图分类号:** TP911.22      **文献标志码:** A      **文章编号:** 1001-3695(2012)04-1497-03

**doi:**10.3969/j.issn.1001-3695.2012.04.082

## Research on channel coding and decoding for DMR standard

LIU Er-xiao, LI Yu-bai, LI Huan

(DSP Laboratory, University of Electronic Science & Technology of China, Chengdu 611731, China)

**Abstract:** For better performance of DMR system, this paper focused on rate 3/4 trellis code and QR (quadratic residue) code in DMR standard. As for the rate 3/4 trellis code, it proposed two different decoding algorithms. One made full use of the characteristics of finite state machine, and the other refined the butterfly computation in viterbi decoding algorithm. It presented a new algorithm to decode QR code by computing the weight of its syndrome polynomial. Simulational results show that the two decoding methods for rate 3/4 trellis code have similar performance, but the first has less computational effort and can be implemented conveniently. Meanwhile, the new algorithm for QR decoding avoids solving the complicated error polynomial and has better performance.

**Key words:** DMR systems; rate 3/4 trellis code; viterbi decode; QR code; weight of syndrome polynomial

### 0 引言

DMR(digital mobile radio)数字专用无线通信系统作为欧洲电信标准协会(ETSI)正在完善的最新数字专业通信标准,在专用无线通信系统迅速发展并逐步从模拟向数字转变的今天,具有很大的研究价值。文献[1]研究了 DMR 标准中的汉明码、RS(reed-solomon)码和多块拓扑码(block product turbo code, BPTC)。文献[2]研究了 DMR 标准中 RS 码的现场可编程门阵列(filed programmable gata array, FPGA)实现。文献[3]分析了 DMR 标准中的各种多块拓扑码的译码。事实上,DMR 标准中还有两种重要的前向纠错码,即网格码和二次剩余码,它们分别在 3/4 率编码数据块和 DMR 系统的语音帧起到非常重要的作用,因而研究这两种编码的译码算法对于开发基于 DMR 协议的新产品具有重要意义。

### 1 Rate 3/4 trellis code

文献[4]规定,DMR 系统中的 3/4 率编码数据包使用 rate 3/4 trellis code。该数据包含有 16 个字节的净荷和 2 个字节的控制数据(7 bit 的数据块序列号和 9 bit 的循环校验码),共 144 个比特,它经过 3/4 率网格编码形成了 DMR 标准帧中的  $96 \times 2 = 192$  个净荷。网格编码是一种有效的纠错码,特别是

维特比译码算法的提出,使其应用越来越广。

#### 1.1 网格编码过程

文献[4]给出了 3/4 率网格编码的具体过程。首先串行输入 144 个比特,然后将其按照从左到右的顺序分成 48 组,每组有串行的三个比特,称为 tribits。在输入的 48 组 tribits 末尾加上  $000_2$  共有 49 组输入。

网格编码器由一个 8 状态的 FSM 组成,其初始状态为 0。从 0 状态开始,当前状态和每组输入按照表 1 映射即可得相应的输出,然后把当前这组输入作为下一个当前状态,依此类推直到第 49 组 tribits 输入完毕。由此得到 49 个位于 0~15 之间的星座点,将它们按照图 1 映射成  $(\pm 1, \pm 3)$  后,再进行交织,最终得到 98 个双比特 dibits。整个编码过程如图 2 所示。

表 1 状态转换表

		input tribits							
		0	1	2	3	4	5	6	7
FSM state	0	0	8	4	12	2	10	6	14
	1	4	12	2	10	6	14	0	8
	2	1	9	5	13	3	11	7	15
	3	5	13	3	11	7	15	1	9
	4	3	11	7	15	1	9	5	13
	5	7	15	1	9	5	13	3	11
	6	2	10	6	14	0	8	4	12
	7	6	14	0	8	4	12	2	10

收稿日期: 2011-08-18; 修回日期: 2011-09-19

作者简介: 刘二晓(1986-),女,河南郑州人,硕士研究生,主要研究方向为集群通信基带算法(xfliu008@sina.com);李玉柏(1965-),男,教授,硕士,主要研究方向为大规模片上网络技术、雷达信号处理;李桓(1978-),男,工程师,硕士,主要研究方向为雷达信号处理、数字集群通信。

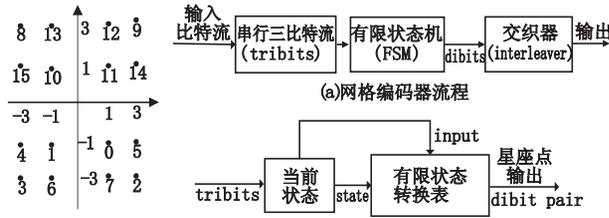


图1 网格编码时各dibits点的星座图

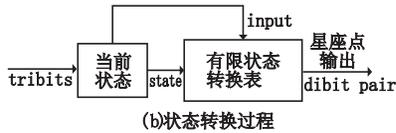


图2 网格编码的原理

1.2 Trellis code 译码过程

网格码的译码原理如图 3 所示。首先要进行解交织和解映射(其中交织和解交织是一个将输入与输出的标号按照固定方式映射的过程,这里不再赘述),然后按照图 1 给出的星座图将 dibits 反映射,得到 49 个 0 ~ 15 的星座点,再按照 FSM 表依次推得前一个状态,得到 49 个十进制表示的 tribits(0 ~ 7),最后再将每个 tribits 用二进制表示即可得到译码输出。所以,译码的关键是根据 FSM 进行状态的反映射。本文提出以下两种译码方案。



图3 网格编码的译码原理

方案 1 充分利用编码过程中状态转换表本身的特性和每个星座点格雷码表示的特点来确定译码输出。具体过程如下:星座点是 0 ~ 15 的十进制数,它们的格雷码如表 2 所示。由表 2 可知,某个星座点被译成与他相邻的数的可能性最大,并且每个星座点仅有一个与之奇偶性不同的相邻点,而在表 1 中每行的奇偶性均相同。因此,如果译码出错,也就是输入的星座点与表 1 中某行的奇偶性不同,找不到与之对应的前一个状态,那么就把与该星座点相邻且奇偶性不同的数作为这一级的译码输出。例如,与 1 相邻的数有 0、3、9,只有 0 与 1 的奇偶性不同,如果译码出错,就把 0 作为这一级的译码输出。方案一的流程如图 4 所示。

表 2 各个星座点的格雷码表示

R	0	1	3	2	6	7	5	4
G	0000	0001	0011	0010	0110	0111	0101	0100
R	8	9	11	10	14	15	13	12
G	1000	1001	1011	1010	1110	1111	1101	1100

方案 2 借鉴 viterbi 译码的思想,先要根据一定的规则计算每一级的分支度量,并记录每一级的前一个状态,最后选择一条与待译码的码字相似度最大的路径作为译码路径。实现时,考虑到译码是从 0 状态开始,根据输入的解映射后的数据判断前一状态,并将其作为当前状态,输入下一个码字,依此类推。为了叙述方便,令 pre\_state 表示前一状态,current\_state 表示当前状态,next\_state 表示下一状态,branch\_metric 表示分支度量,path\_metric 表示路径度量。

根据本系统的特点将 viterbi 译码算法作如下改进:假设每个由 current\_state 和输入的星座点推断出 next\_state 的过程为一级,从 FSM 表可知,DMR 系统中的网格编码每一级有 0 ~ 7 八个状态,且每个状态可能来自于上一级的八种状态。因此每一级要计算由前一级的八个状态到这一级的每个状态的 branch\_metric,然后选择最小 branch\_metric 所对应的那个状态作为当前这一级 current\_state 的 pre\_state。如此类推,一直计算到第 49 级,共得到八条路径,从最后一级开始回溯,根据各

个状态所记录的 pre\_state,找到这八条路径,将各级的 branch\_metric 加起来得到各自的 path\_metric,选择 path\_metric 最小的一条路径作为译码路径。其中分支度量是按照图 1 中各个星座点之间的几何距离来计算的。例如,当前状态是 0,输入是 0,那么就计算前一状态 0 ~ 7 的各点(0,4,1,5,3,7,2,6)到 0 几何距离分别是 0,4,2,2,√5,2,2√2,2√2,选择其中最小的一个为 0,对应的状态为 0,这样就记录下这一级的前一状态 0 和分支度量 0。具体流程如图 5 所示。

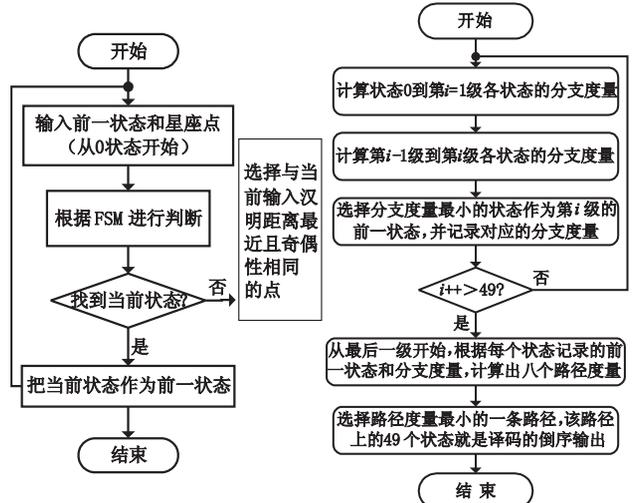


图4 Trellis Code解码方案1

图5 Trellis Code解码方案2

1.3 仿真结果及分析

按照图 6 的流程对以上两种方案在 MATLAB 下进行仿真,结果如图 7 所示。从仿真结果可以看出,两种方案的性能在不同的信噪比下没有太大区别。从计算复杂度来看,方案 1 根据表 1 和 2 可以直接得到每一级的译码输出,不需要记录;而方案 2 每一级都要计算八个分支度量并记录其中最小一个,还要计算八个路径度量选择其中最小一个确定译码路径,译码结束至少需要 392 次平方和运算和 392 次加法运算,还需要足够的空间来保存每一级记录下来的分支度量。因此,方案一的计算量少,所需的存储空间小,更适合工程应用。

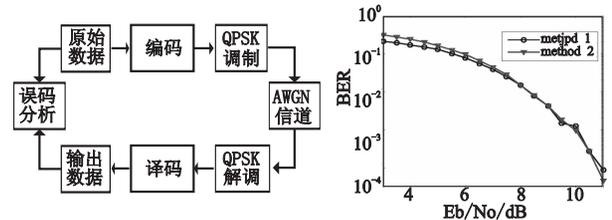


图6 MATLAB性能仿真框图

图7 Trellis Code的译码性能图

2 QR 码

文献[4]中规定,DMR 标准中的语音帧有 32 bit 的嵌入信令域(embedded signaling field, EMB),它要求使用 QR(16,7,6)码作为其前向纠错码(FEC),并分配在 EMB 的左右 8 bit 位置。QR(quadratic residue)码被称为二次剩余码,是一类具有高效纠错能力的循环码。

2.1 QR 码的构成

QR 码是长度为一个素数 p 的 GF(l)上的循环码,其中 l 是 mod p 的平方剩余。对于 l=2 的二元平方剩余码,码长 p 是形如 8m ± 1 的素数。设 Q 是 mod p 的平方剩余数的集合,即

$$Q = \{i | i \equiv j^2 \pmod p, j=1,2,\dots,p\} \quad (1)$$

由于  $l \in Q$ , 所以  $Q$  在乘  $l$  运算下封闭, 并且  $Q$  还可以表示成  $\text{mod } p$  的不交分圆陪集的并, 如式(2)所示:

$$Q = \bigcup_{r \in S} Q_r \quad (2)$$

其中:  $S$  为分圆陪集的代表元的集合, 称为基集;  $Q_r$  表示代表元  $r$  所在的陪集, 如式(3)所示:

$$Q_r = \{r^j | j=0,1,\dots,P_r-1\} \quad (3)$$

其中:  $P_r$  是满足  $r^{P_r} \equiv r \pmod p$  的最小正整数。

设  $g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^l)$  为 QR 码的生成多项式, 则  $g(x)$  的系数属于  $GF(l)$ 。其中,  $\alpha$  是  $GF(l)$  的某个扩域的本原  $p$  次单元根。由  $g(x)$  生成的码长为  $p$  的  $GF(l)$  上的循环码称为二次剩余码。对于 QR(17,9,5), 有  $Q = \{1,2,4,8,9,13,15,16\} = Q_1$ 。

### 2.2 QR 码的代数译码

二次剩余码的代数译码方式有很多种, 一般包含两个部分: a) 用某种方法求出错误位置多项式的系数; b) 求出错误位置多项式的根以确定错误位置。

设  $c$  为发送码字, 经过有噪信道得到  $r = c + e$  为接收码字。令校验多项式  $s_1(x) = r(x) \pmod{g(x)}$ , 其中  $h_i^{(1)} \equiv x_i \pmod{g(x)}$ , 将  $s_1$  变换得到  $s_2$ , 可得式(4)(5):

$$s_1 = r [h_0^{(1)} \quad h_1^{(1)} \quad \cdots \quad h_{n-1}^{(1)}]^T = e [h_0^{(1)} \quad h_1^{(1)} \quad \cdots \quad h_{n-1}^{(1)}]^T \quad (4)$$

$$s_2 = r [h_{\text{deg}(g(x))}^{(1)} \cdots h_{n-1}^{(1)} \quad h_0^{(1)} \cdots h_{\text{deg}(g(x))-1}^{(1)}]^T = e [h_{\text{deg}(g(x))}^{(1)} \cdots h_{n-1}^{(1)} \quad h_0^{(1)} \cdots h_{\text{deg}(g(x))-1}^{(1)}]^T = e [h_0^{(2)} \quad h_1^{(2)} \quad \cdots \quad h_{n-1}^{(2)}]^T \quad (5)$$

其中:  $\text{deg}(g(x))$  表示多项式  $g(x)$  的最高次数, 为了叙述方便, 令  $\text{deg}(g(x)) = D$ , 并作以下假设:

$$\begin{cases} T_1 = [h_0^{(1)} & h_1^{(1)} & \cdots & h_{n-1}^{(1)}]^T \\ T_2 = [h_0^{(2)} & h_1^{(2)} & \cdots & h_{n-1}^{(2)}]^T \end{cases} \quad (6)$$

$$\begin{cases} h_i^{(1)}(x) = a_{i,0}x^0 + a_{i,1}x^1 + \cdots + a_{i,D-1}x^{D-1} \\ h_i^{(2)}(x) = a_{i,0}x^0 + a_{i,1}x^1 + \cdots + a_{i,D-1}x^{D-1} \end{cases} \quad (7)$$

$$\begin{cases} wt(T_{1,i}) = wt(a_{i,0}, a_{i,1}, \dots, a_{i,D-1}) \\ wt(T_{2,i}) = wt(a_{i,0}, a_{i,1}, \dots, a_{i,D-1}) \end{cases} \quad (8)$$

其中:  $a_{i,0}, a_{i,1}, \dots, a_{i,D-1} \in GF(2), i=0,1,\dots,n-1$ ;  $wt(T_{1,i}), wt(T_{2,i})$  分别表示  $T_1 - T_2$  中第  $i$  行的码重。

由于  $h_i^{(1)} \equiv x^i \pmod{g(x)}$ , 所以当  $i < D$  时,  $h_i^{(1)} \equiv x^i \pmod{g(x)} = x^i$  即  $wt(T_{1,i}) = 1$ ; 当  $i \geq D$  时,  $h_i^{(1)} \equiv x^i \pmod{g(x)}$  表明  $x^i + h_i^{(1)}(x)$  可以被  $g(x)$  整除, 即它是一个码字  $C$ 。因此满足  $wt(T_{1,i}) + 1 \geq d$ , 即  $wt(T_{1,i}) \geq d - 1$  ( $d$  表示该 QR 码的最小码重)。所以, 当且仅当  $i < D$  时,  $wt(T_{1,i}) \geq d - 1$ ; 同理, 当且仅当  $i \geq D$  时,  $wt(T_{2,i}) \geq d - 1$ 。

设  $e = (e_0, e_1, \dots, e_{n-1})$  是可纠正的错误类型, 即接收码字中错误个数不超过  $t$  ( $t$  为该 QR 码可以纠正的最大错误比特数)。因此, 如果所有的错误比特都发生在前半部分或者后半部分, 那么可以通过分别计算校验多项式  $s_1$  和  $s_2$  的码重来确定错误位置; 否则, 需要分别在  $s_1$  和  $s_2$  加上一个矢量以保证所有的错误都发生在相同的半部。

例如, QR 码满足最小码距  $d$  和纠错个数  $t$  之间的关系:  $d \geq 2t + 1$ 。对 QR(17,9,5) 来说, 它的最小码重  $d = 5$ , 因此最大纠错个数  $t = 2$ 。若其错误多项式为  $e(x) = x^1 + x^5$ , 则  $s_1 =$

$h_1^{(1)} \oplus h_5^{(1)}$  为伴随多项式, 这时把  $h_5^{(1)}$  加到  $s_1$  上可得  $s_1 \oplus h_{10}^{(1)} = (0100000000000000)$ , 故  $wt(s_1 \oplus h_{10}^{(1)}) = 1$ , 这样便可确定错误位置  $i = 2$ 。按照这个思路可得 QR(17,9,5) 的译码流程如图 8 所示。将 QR(17,9,5) 的末位加上一个奇偶校验位, 扩展为 QR(18,9,6), 再将其前面两位位置 0, 即可得到 DMR 标准中使用的 QR(16,7,6) 码。

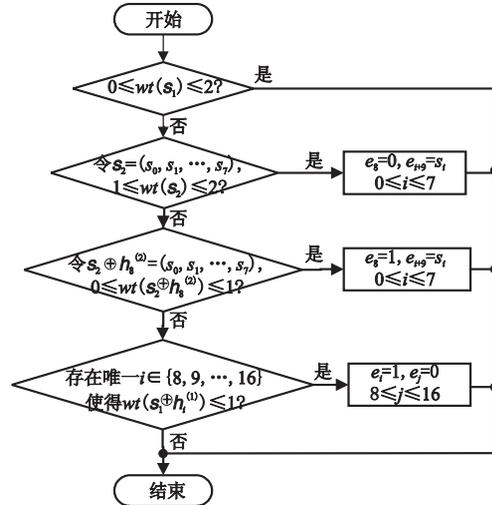


图8 QR(17,9,5)的译码流程

### 2.3 仿真结果及分析

文献[5]给出了一种基于牛顿等式的 QR(17,9,5) 译码方法, 其主要思路如下: 假设  $s_1$  表示伴随多项式, 若  $s_1 = 0$ , 则表明信息位无错; 若  $s_1^{17} = 1$ , 则接收码字中存在一个错误,  $s_1$  标志错误位置; 若  $s_1^{17} \neq 1$ , 则接收码字中至少存在两个错误, 如果方程  $x^2 + s_1x + s_1^{15} = 0$  在  $\{1, \alpha, \dots, \alpha^{16}\}$  中存在两个不同的解, 设为  $\alpha^i - \alpha^j$ , 则表示第  $i$  位和第  $j$  位有错; 否则接收多项式中存在三个以上错误。

根据以上原理, 在 MATLAB 下对 QR(16,7,6) 译码过程按照图 6 进行仿真, 其结果如图 9 所示。Method1 采用文献[5]中的方法, method2 采用本文介绍的方法。

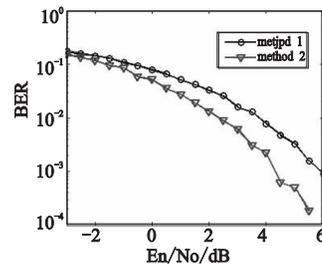


图9 QR 码的译码性能

从图 9 可看出, 与文献[5]中的方法相比, 本文方法的译码性能提高了 1.5 dB。从计算复杂度的角度来说, 该算法仅涉及与和异或操作。在最坏的情况下, 该方法仅需要 170 次异或和 204 次与运算, 而文献[5]的方法在错误比特大于 1 时, 要求解 16 阶方程  $x^2 + s_1x + s_1^{15} = 0$  的根。该方程是有限域上的方程, 其根只能是  $\{1, \alpha, \dots, \alpha^{16}\}$  中的两个, 求解时要将每个位置对应的可能的根代入方程进行验证。如果方程成立, 那么该元素就是方程的根, 否则继续尝试下一个错误位置, 直到找到方程所有的根。在最坏的情况下, 该算法需要 408 次乘法和 272 次加法运算。因此, 本文的方法更适合工程应用。

整个网络中只有一台主机感染了蠕虫,即  $I(0) = 1$ ,其余主机均是易感染主机。基于KM得到CodeRed在A、B网络中的传播速度仿真结果分别如图3、4所示。

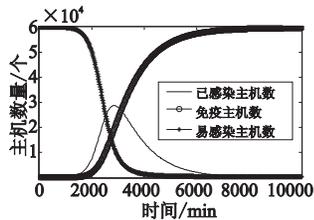


图3 A网CodeRed实验仿真结果

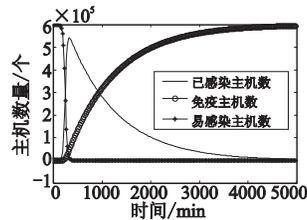


图4 B网CodeRed实验仿真结果

### 3.2 基于DLM的V6-Worm传播仿真分析

再将3.1节的两个网络移植到IPv6中,由于V6-Worm在子网内采用基于MLD扫描的扫描发现算法,在子网间采用基于BGP路由前缀信息的扫描算法,通过2.2节的分析可知,子网间要扫描的地址空间为 $2^{54}$ ,则子网间感染率可假设为 $K/2^{54}$ 。假设V6-Worm与CodeRed具有相同的扫描速度, $q = 0.5$ ,A网络划分为60个子网,B网络划分为600个子网,主机恢复率 $\gamma = 0.001$ ,子网恢复率 $\sigma = 10^{-5}$ , $J(0) = 1$ ,在本地子网的延迟为 $\xi = 1$  min,其他参数不变,基于DLM得到V6-Worm的传播速度仿真结果如图5、6所示。

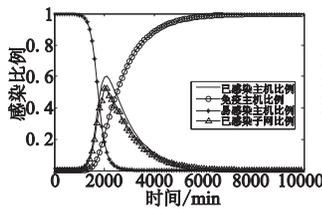


图5 A网V6-Worm实验仿真结果

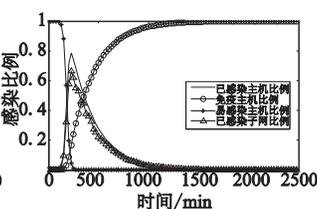


图6 B网V6-Worm实验仿真结果

### 3.3 仿真结果分析

图3、4仿真结果显示,CodeRed在IPv4网络的A网传播过程中,在2800 min左右达到传播的顶峰,而在B网传播过程中,在400 min左右到达顶峰。由图5、6仿真结果显示,V6-Worm在IPv6网络的A网传播过程中,在2100 min左右达到传播的顶峰,而在B网中传播时,大约260 min达到传播顶峰。可见,V6-Worm是能够在IPv6网络中传播的,随着主机总数的增加,V6-Worm传播速度明显加快,同时,其传播速度要明显

快于CodeRed的传播速度。

## 4 结束语

本文构建了一种IPv6蠕虫——V6-Worm,根据V6-Worm的双层扫描策略,基于KM模型构建了DLM模型,通过仿真实验,认为在IPv6网络中,运用双层扫描策略,V6-Worm能够在IPv6网络中传播,其传播速度甚至要快于采用随机扫描策略的CodeRed的传播速度。本文的DLM传播模型是在KM模型基础上改进而来的,其中所有主机处于易感染状态、已感染状态和免疫状态中的一种。但是,KM模型没有考虑易感染主机被补丁升级和人为对抗蠕虫传播的情况,因此,后续的研究工作将着重在TFM传播模型的基础上构建TLM模型。

### 参考文献:

- [1] CERT. CERT/CC advisories [EB/OL]. (2002-05-15) [2011-08-28]. <http://www.cert.org/advisories/>.
- [2] ZOU C C, TOWSLEY D, GONG Wei-bo, *et al.* Routing worm: a fast, selective attack worm based on IP address information [C]//Proc of the 19th Workshop on Principles of Advanced and Distributed Simulation. Washington DC: IEEE Computer Society, 2005: 199-206.
- [3] HINDEN R, DEERING S. RFC 4291, IP version 6 addressing architecture[S]. [S. l.]: Network Working Group, 2006.
- [4] 刘煜,郑庆华,管晓宏,等. IPv6网络中蠕虫传播模型及分析[J]. 计算机学报,2006,29(8):1337-1345.
- [5] 卿斯汉,王超,何建波,等. 即时通信蠕虫研究与发展[J]. 软件学报,2006,17(10):2118-2130.
- [6] 徐延贵,钱焯延,张凯. IPv6网络中的DNS蠕虫研究[J]. 计算机科学,2009,36(12):32-36.
- [7] VIDA R, COSTA L. RFC 3810, Multicast listener discovery version 2 (MLDv2) for IPv6[S]. [S. l.]: Network Working Group, 2004.
- [8] Company ID list of IEEE [EB/OL]. (2011-08-31). <http://standards.ieee.org/regauth/oui/oui.txt>.
- [9] 徐延贵,钱焯延,李华峰. IPv6网络中的路由蠕虫传播模型[J]. 计算机应用研究,2009,26(10):3918-3924.
- [10] ZOU Chang-chun. The monitoring and early detection of Internet worms [J]. IEEE/ACM Trans on Networking,2005,13(5):961-974.

(上接第1499页)

## 3 结束语

本文对传统的译码方法进行改进后,提出了分别适用于DMR系统中3/4率网格码和二次剩余码的新译码方法,新方法具有性能好、计算量小等优点。下一步工作的重点是将本文提出的译码算法在DSP平台上实现,再从执行速度、存储空间等方面对其进行优化改进。

### 参考文献:

- [1] 代敏. DMR系统的信道编码研究[D]. 西安:西安电子科技大学,2008.
- [2] 宋洋军,权进国,林孝康. DMR标准RS码编译码器的FPGA实现[J]. 通信技术,2010,43(6):32-35.
- [3] 刘辉,谢晓明. 基于DMR通信协议的信道编码的研究[J]. 现代电子技术,2009,23(9):37-39.
- [4] Electromagnetic compatibility and radio spectrum matters (ERM),

Digital mobile radio (DMR) systems, Part 1: DMR air interface (AI) protocol, ETSI TS 102 361-1 V1.4.5[R]. 2007.

- [5] 马建峰,王育民. 二次剩余码的有效译码[J]. 西安电子科技大学学报,1996,23(3):295-302.
- [6] 谢永军. 基于DMR数字集群通信技术的研究[D]. 北京:北京邮电大学,2009.
- [7] SANDHU S, HEATH R, PAULRAJ A. Space-time block codes versus space-time trellis codes [C]//Proc of IEEE International Conference Communications. 2001:1132-1136.
- [8] SHI Jun, WESEL R D. Further error event diagram reduction using algorithmic techniques [C]//Proc of IEEE International Conference on Communications. 2003:2822-2826.
- [9] TRUONG T K, SHIH P Y, SU Wen-ku, *et al.* Algebraic decoding of the (89,45,17) quadratic residue code [J]. IEEE Trans on Information Theory,2008,54(11):5005-5011.
- [10] CHANG Y, LEE C D, CHEN Z H, *et al.* (23,12,7) quadratic residue decoder based on syndrome-weight determination [J]. Electron Letter,2008,44(19):1147-1149.