文章编号:1001-506X(2010)01-0195-05

认知系统 AES-LDPC 纠错加密器的设计与性能分析

鲁凌云[1],肖 扬[1],姜月秋[2],宋丽丽[1]
(1. 北京交通大学信息科学研究所,北京 100044;
2. 沈阳理工大学信息通信工程学院,辽宁 沈阳 110168)

摘 要:在多跳的认知系统中,由于不存在可信实体作为服务器控制密钥分发,安全性将面临更大挑战,需要建立完善的加密体系结构来解决这一问题。将高级加密标准 AES 和在通信纠错领域性能优异的低密度奇偶校验码(low-density parity-check, LDPC)结合,设计出了分组长度为 128 bit 的六轮宽轨迹加密策略、密钥由 128 bit AES 密钥和 LDPC 生成矩阵组成的 LDPC 纠错加密器。由于 LDPC 生成矩阵具有更好的扩散性能,使得这种新设计的 LDPC 纠错加密器能在更少的轮数下具有较好的安全性。最后,通过实验结果验证了 AES-LDPC 纠错加密器的性能。

关键词:认知无线电;高级加密标准;LDPC 编码;交织干扰器
中图分类号:TN 911.2 **文献标志码**:A

Design and performance analysis of AES-LDPC error correcting cipher for cognitive radio systems

LU Ling-yun[1], XIAO Yang[1], JIANG Yue-qiu[2], SONG Li-li[1]
(*1. Inst. of Information Science, Beijing Jiaotong Univ., Beijing 100044, China;*
2. Coll. of Computer and Communication, Shenyang Inst. of Technology, Shenyang 110168, China)

Abstract: In the hopping cognitive radio (CR) system, the security is facing a challenge because there does not exist that a server as the credible entity to display the keyboard. So it is necessary to enhance the encrypting system to solve the problem. The paper presents an LDPC error correcting cipher by combining the advanced encryption standard (AES) and LDPC code. The LDPC error correcting cipher, which is based on wide trail strategy, is a six round block cipher that encrypts 128 bit plaintexts, and the key is composed of 128 bit AES secret keys and an LDPC generator matrix. By using the LDPC generator matrix with high performance in the property of diffusion, the LDPC error correcting cipher has a fairly good property in security in fewer rounds. Simulation results show that the processes of encrypting/decrypting have the better performance.

Keywords: cognitive radio; advanced encryption standard; LDPC channel coding; interleaving jammer

0 引 言

认知无线电 (cognitive radio,CR)是 1999 年由 Joseph Mitola 提出的一种新智能无线通信技术[1],CR 能够在一些授权频段未使用的情况下使用该频段进行通信,并且能够在时域、频域和空域多维空间自动调整发射及接收参数[2]。CR 系统与传统无线通信的数据处理方式之间的区别如图 1(a)和图 1(b)所示。由于 CR 系统加入了认知模块,因此认知无线电除具有传统无线通信的安全问题,还引发了一些新的安全隐患,如对主用户的冒充等。此外,由于多跳 CR 系统中不存在可信实体作为服务器控制密钥材料分发,安全将面临更大挑战,需要建立完善的密钥管理体系结构来解决这一问题。因此,虽然关于 CR 系统的安全性问题尚处于初步研究阶段,但随着系统的不断发展和完善,信息安全问题将成为认知网能否应用于实际中的主要瓶颈之一[3-4]。

收稿日期:2008-11-06; **修回日期**:2009-10-14。
基金项目:国家自然科学基金(60572093)资助课题
作者简介:鲁凌云(1977-),女,讲师,博士,主要研究方向为网络通信协议、无线通信信号处理技术。E-mail:lylu@bjtu.edu.cn

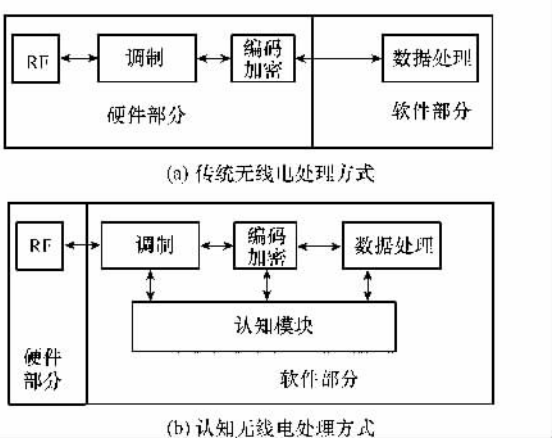

图 1 传统无线电处理方式与认知无线电处理方式

重要信息在认知系统中的传输不仅要有很好的保密性,而且还要有一定的容错性能。如图 1 所示,信息加密后需要将加密信息送到编码信道,通过纠错编码使密码具有一定的容错能力[5-7]。但是,这种分两步操作的方法存在如下问题:一是增加了系统的复杂性;另外使得系统产生较大的时延。如果纠错和加密方法的设计没有很好的结合,CR 系统的纠错能力和安全性都会受到很大程度的影响。本文根据认知系统设计了一个六轮循环的分组低密度奇偶校验码(low-density parity-check, LDPC)纠错加密器,结合了 LDPC 码的高扩散性、纠错能力强和高级加密标准(advanced encryption standard, AES)安全性高等特点[8-9],将 128 位 AES 密钥和 LDPC 码生成矩阵/校验矩阵作为密钥提供给合法认知系统中的主用户,因此具有较高的安全性和数据纠错能力。

1 AES-LDPC 纠错加密器的设计

1.1 AES-LDPC 扩散码的设计

LDPC 纠错加密器的前五轮使用了 AES 密码的行移位变换和列混淆变换扩散操作,在第六轮使用了一个 256×512的 LDPC 生成矩阵。行移位变换是在中间密文状态的每行上运算,对于 128 bit 的分组长度采用如下变换

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,3} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{bmatrix} \tag{1}$$

式(1)运算实际上是一个换位密码,重排了元素的位置而不改变元素本身,第 $i(i=0,1,2,3)$行的元素,位置重排就是"循环向右移动"$4-i$ 位。式(2)矩阵则对每一列采用已知密钥的一个多表代换(乘积)密码代数式,即

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} c_0 & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_3 & c_2 \\ c_2 & c_1 & c_0 & c_3 \\ c_3 & c_2 & c_1 & c_0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} '02' & '03' & '01' & '01' \\ '01' & '02' & '03' & '01' \\ '01' & '01' & '02' & '03' \\ '03' & '01' & '01' & '02' \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \tag{2}$$

与 AES 加密过程相同,LDPC 码的前五轮使用了混淆变换,即 $R_5=4^5$,LPDC 编码的扩散传播码为 $R_{\mathrm{LDPC}}=256=4^4$。因此,LDPC 纠错加密器的扩散传播码率为

$$R = R_5 \times R_{\mathrm{LDPC}} = 4^5 \times 256 = 4^9 \tag{3}$$

1.2 无四环随机 LDPC 纠错加密密码的构造

单纯的通过 LDPC 纠错加密器是无法有效保证系统的纠错性能,为此本文构造了具有快速收敛、解码延迟小等特点的无四环随机 LDPC 码。此纠错密码的特点是:随机 LDPC 码具有最小码重和码间距离近似为码长的线性函数的优点,使得通过代数方法构造的 QC LDPC 码的环特性、距离特性和误码率性能上很难优于或接近随机 LDPC 码;此外,随机 LDPC 码比 QC LDPC 码更安全,密码攻击者很难攻击随机 LDPC 码。

设 $M\times N$ 的校验矩阵为

$$\boldsymbol{H} = \begin{bmatrix} h(1,1) & h(1,2) & \cdots & h(1,N) \\ h(2,1) & h(2,2) & \cdots & h(2,N) \\ \vdots & \vdots & & \vdots \\ h(M,1) & h(M,2) & \cdots & h(M,N) \end{bmatrix} = [\boldsymbol{h}(1) \cdots \boldsymbol{h}(N)] \tag{4}$$

任取两列向量 $\boldsymbol{h}(i)=[h(1,i) \cdots h(M,i)]^{\mathrm{T}}$ 和 $\boldsymbol{h}(j)=[h(1,j) \cdots h(M,j)]^{\mathrm{T}}$,$j\neq i$ 当且仅当满足 $\boldsymbol{h}^{\mathrm{T}}(i)\boldsymbol{h}(j)<2$,校验矩阵(4)应无四环。因此,根据下列步骤构造无四环的随机 LDPC 码。其中,校验矩阵的行重为 6,列重为 3。

步骤 1 将 3 个 1 随机地放置在校验矩阵第一列上,得到 $\boldsymbol{h}(1)=[h(1,1) \cdots h(M,1)]^{\mathrm{T}}$;

步骤 2 将 3 个 1 随机地放置在校验矩阵第二列上,得到 $\boldsymbol{h}(2)=[h(1,2) \cdots h(M,2)]^{\mathrm{T}}$,检验是否满足 $\boldsymbol{h}^{\mathrm{T}}(1)\boldsymbol{h}(2)<2$;如果不满足,重新将 3 个 1 随机地放置在校验矩阵的第二列上,直到满足 $\boldsymbol{h}^{\mathrm{T}}(1)\boldsymbol{h}(2)<2$;

步骤 3 将 3 个 1 随机地放置在校验矩阵第 i 列上,得到 $\boldsymbol{h}(i)=[h(1,i) \cdots h(M,i)]^{\mathrm{T}}$,检验是否满足下式

$$\boldsymbol{h}^{\mathrm{T}}(i)\boldsymbol{h}(j) < 2,\ j = 1,\cdots,i-1 \tag{5}$$

和 $\boldsymbol{H}_i$ 的行重大于 0 并小于或等于 6,其中

$$\boldsymbol{H}_i=\begin{bmatrix} h(1,1) & h(1,2) & \cdots & h(1,i) \\ h(2,1) & h(2,2) & \cdots & h(2,i) \\ \vdots & \vdots & & \vdots \\ h(M,1) & h(M,2) & \cdots & h(M,i) \end{bmatrix}= \begin{bmatrix} \boldsymbol{h}(1) & \cdots & \boldsymbol{h}(i) \end{bmatrix} \tag{6}$$

如果不满足,重新将 3 个 1 随机地放置在校验矩阵第 i 列上,直到满足式(5)和 $\boldsymbol{H}_i$ 的行重条件。

2　认知无线电 AES-LDPC 的加密与解密

假定主用户数据流 $u_{\mathrm{PU}}(k)(k=1,2,\cdots,K)$,次用户数据流 $u_{\mathrm{CR}}(k')(k'=1,2,\cdots,K')$,生成矩阵 $\boldsymbol{G}=\begin{bmatrix} G_k \vdots \\ G_{k'} \vdots \end{bmatrix} \boldsymbol{I}_{M\times M}$,编码后码字 $c(v)(v=1,2,\cdots,V)$,LDPC 纠错加密器中取 $P=256$,$Q=512$,则

$$\begin{bmatrix} c(1) & c(2) & \cdots & c(V) \end{bmatrix}= \begin{bmatrix} u_{\mathrm{PU}}(1) & \cdots & u_{\mathrm{PU}}(K) & u_{\mathrm{CR}}(1) & \cdots & u_{\mathrm{CR}}(K') \end{bmatrix} \begin{bmatrix} g_{\mathrm{PU}11} & \cdots & g_{\mathrm{PU}1K} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ g_{\mathrm{PU}K1} & \cdots & g_{\mathrm{PU}KK} & 0 & \cdots & 1 \\ g_{\mathrm{CR}11} & \cdots & g_{\mathrm{CR}1K'} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ g_{\mathrm{CR}K'1} & \cdots & g_{\mathrm{CR}K'K'} & 0 & \cdots & 1 \end{bmatrix}_{P\times Q} \tag{7}$$

根据式(7)可知,当消息序列有一个比特的变化时,将会引起 256(一半码字)bit 的变化。导致消息空间出现冗余的统计结构具有很好扩散性的密码加密消失在密文里,在量化概念上每一位明文和密钥 bit 将会影响密文 bit 的数量,1 bit的明文变化会引起 256 位密文状态的改变。基于认知系统的 LDPC 纠错加密机器是一个输入为 256 位,密钥为 128 位 AES 密钥和 LDPC 码生成的校验矩阵,输出为 512 位的分组密码。

如图 2 所示,系统由 AES-LDPC 纠错密码编码器和一些必需的辅助模块,如交织干扰器、密钥管理接口等组成。交织干扰器的作用是减少数据冗余,以及给LDPC码的信息位向量加密。由于 LDPC 码有两个向量,即校验位向量和信息位向量。生成矩阵的变化不会影响到信息位向量,所以交织器可以完成信息位向量的加密后,用正交交织器混淆 LDPC 纠错编码器加密后的码字。在 LDPC 纠错密码编码器之后,连接一个交织干扰器。由 LDPC 编码的性质知道,在 LDPC 纠错密码编码器之后连接一个交织器混淆位置信息,进一步加强密码抵抗密码攻击的性能。因此,此加密系统由 128 位轮密钥,LDPC 码 256×512 校验矩阵 $\boldsymbol{H}$ 和交织图组成。认知用户少得到其中的任何一个密钥都不能完成对密文的解密,也就无法获得正确的数据。密钥管理接口的作用就是管理、发送和存储这些密钥。LDPC 纠错密码解码器是 LDPC 纠错密码加密器的反过程,解交织干扰器的功能是解除交织器的交织加密。这里的解交织器是与加密系统中交织器相匹配的类型。

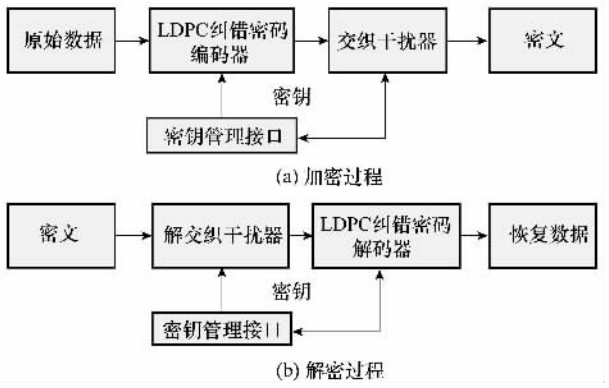

图 2　AES-LDPC 加密器的加密和解密过程

3　安全性分析

3.1　线性差分攻击的抵抗性

假定设计的 LDPC 纠错加密器,前 5 轮循环活动字节的 AES 扩散传播率为 4,密码替换层的 S 盒的最大传播比为 2^{-6},最小输入输出的相关性为 2^{-3}。因此,前五轮的差分轨迹传播分析的复杂度将稍小于 $O(2^{128})$。但是由于在 LDPC 纠错加密器的最后一轮使用了 256×512 的生成矩阵,这远远大于 AES 轮函数的扩散传播率,LDPC 纠错加密器的差分轨迹传播比将远远小于 2^{-127},即差分分析的复杂度将远远大于 $O(2^{128})$。同理,前五轮的输入输出相关性为 2^{-60} 也稍大于 2^{-64},意味着线性分析的复杂度将稍小于 $O(2^{128})$。LDPC 纠错加密器的输入输出相关性远远小于 2^{-127},即线性分析的复杂度将远远大于 $O(2^{128})$。

3.2　随机 LDPC 码的抵抗性

从另一个角度,对本文设计的随机 LDPC 码的算法复杂度可以通过如下定理估算出密码分析攻击 LDPC 码的安全性能。

定理 1　随机 LDPC 码抵抗性的评估性能为优,当且仅当 $\boldsymbol{H}$ 矩阵时间复杂度为 $C=2^{3\,289}$,远大于 2^{128}。

证明　通过对随机 LDPC 码算法的描述,可以进行如下推导:

第一列 1 放置的可能性,$C_{256}^{3}=2\ 763\ 520$;

第二列 1 放置的可能性,$C_{256}^{3}-C_{3}^{2}-C_{3}^{3}=C_{256}^{3}-4=2\ 763\ 516$;

第三列1放置的可能性,$C_{256}^{3}-2\times(C_{3}^{2}+C_{3}^{3})=C_{256}^{3}-8=2\ 763\ 512$;

⋮

第 N 列 1 放置的可能性，$C_{256}^{3}-(N-1)\times(C_{3}^{2}+C_{3}^{3})=C_{256}^{3}-4\times(N-1)$。

通过计算得到攻击者猜测出 $\boldsymbol{H}$ 矩阵的需要的时间复杂度 $C=10^{3\,289}$，我们可以看到 $10^{3\,289}>2^{128}$，而且是远大于 2^{128}。因此，我们在 LDPC 纠错加密器中使用了随机 LDPC 编码使得密码分析复杂度大大提升，保证了 LDPC 纠错加密器具有很高的安全性。

4 性能仿真

通过仿真实验来检测加密效果，这里使用一幅图像作为加密数据源，实际应用中也可以是其他类型的数据。假设加密数据包是在认知无线电系统传输过程中被 CR 用户截获的，通过比较加密数据与原始数据，可以检验出加密效果。由于本文提出的加密 LDPC 编解码器也有纠错和抗干扰的功能，可将原始数据和强噪声条件下的解密数据相比较来检验性能。要破解本方案加密以后的图像，需要进行下面的工作：一方面需要得到加密所使用的置乱矩阵；另一方面需要得到用于加密的伪随机序列。本节将从以下几个方面进行性能仿真测试：

(1) 测试 LDPC 纠错密码加密效果；

(2) 测试 CR 用户解密效果；

(3) 测试 LDPC 纠错密码对信道的抗干扰能力。

4.1 加密性能的测试

如图 3～图 9 所示，假设 256×256 一副图像 A1 作为原始数据，经 LDPC 纠错加密器加密后图像为 B1；CR 用户在没有获得 128 bit AES 密钥时解密图像 C1，CR 用户在没有获得随机 LDPC 校验矩阵时解密图像 C2；采用 BPSK 调制，信道为 AWGN 信道，在信噪比别为 2.5 dB/2.9 dB/3 dB，AES-LDPC 纠错加密系统解码后图像 D1/D2/D3。

图 3 原始图像 A1

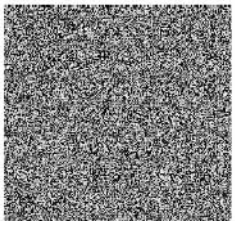

图 4 LDPC 纠错加密器加密后图像 B1

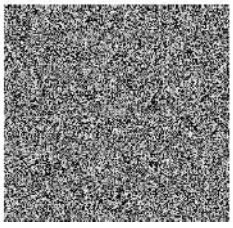

图 5 CR 用户没有获得 128 bit 密钥时恢复图像 C1

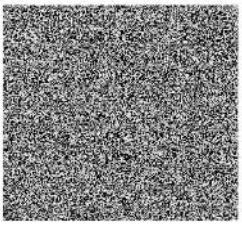

图 6 CR 用户没有获得 $\boldsymbol{H}$ 矩阵解密后图像 C2

图 7 信道信噪比位 2.5 dB 时恢复图像 D1(BER=1.6e−3)

图 8 信道信噪比为 2.9 dB 时恢复图像 D2(BER=2.670 3e−4)

图 9 信道信噪比为 3 dB 时恢复图像 D3(BER=0)

仿真实验结果证明，使用 AES-LDPC 纠错加密机具有很好的加密效果，同时也表明认知用户得不到密钥，解密的图像几乎无法恢复原始图像。此外，在信道信噪比大于等于 3 dB 时，合法用户都能准确无误地恢复原始数据。

4.2 BER 性能测试

我们分别选择了 10^5 和 10^6 两个子集对其码重分布进行统计，实验结果如图 10 和图 11 所示，结果表明用本文方法构造的 LDPC 纠错密码的码重分布集中在 120 附近，码重小于 90 的数目只占测试数目的 0.16% 和 0.24%，而最小码重则集中在 70 附近，这说明 AES-LDPC 纠错加密器的纠错能力并没有大幅下降，在提供安全性的同时很好地保证了系统的传输性能。

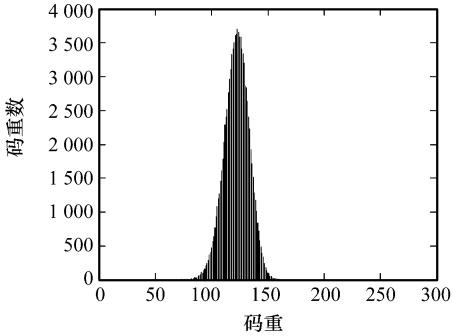

图 10 统计 10^5 个码字得到的码重(最小码重 72)

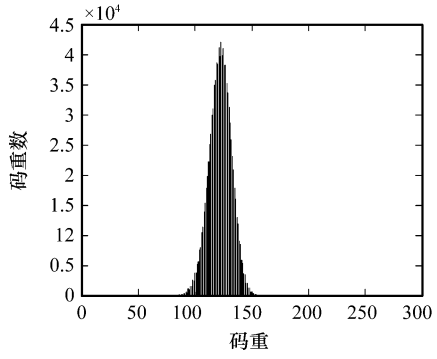

图 11　统计 10^6 个码字得出的码重(最小码重 66)

图 12 给出了 AES-LDPC 纠错加密器在信噪比从 0 dB 到 5 dB 增加的过程中的 BER 性能。不难发现,如果系统的 BER 达到 10^{-2} 需要 2 dB;如果系统的 BER 达到 10^{-3} 需要 3 dB。

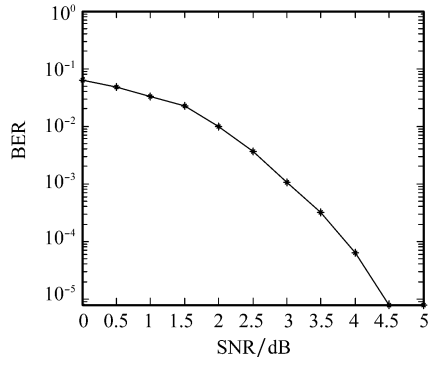

图 12　LDPC 纠错密码的 BER 性能示意图

4.3　系统处理速度

如表 1 所示,对 AES-LDPC 纠错加密算法的加密/解密处理速度与传统的 AES 加密算法进行了对比分析。

表 1　AES-LDPC 纠错加密算法与 AES 加密算法

算法名称	密钥的安装速度/(Mbit/s)	加密速度/(Mbit/s)	解密速度/(Mbit/s)
AES	8.54	10.21	9.87
AES-LDPC	6.78	9.01	8.75

从表 1 中可以看出,虽然密钥的安装速度、加密速度、解密速度等方面略慢一些,但是综合考虑各方面因素,对于 CR 系统需要的安全性高,并且需要对大量的数据进行加密,因此 AES-LDPC 纠错加密器将是较好的选择。

5　结　论

本文提出了一种 LDPC 纠错加密器,密钥由 128 位 AES 密钥和 LDPC 码生成/校验矩阵组成,它对 256 位明文加密生成 512 位密文。通过理论分析和实验仿真表明具有很高的安全性能和纠错性能。本文也给出了 LDPC 纠错密码加密和解密的方法。实验证明使用本文设计的 LDPC 纠错密码对消息加密,在信道信噪比大于等于 3 dB 时,都能准确无误地恢复原始数据。

参考文献:

[1] Mitola Joseph. Cognitive radio: an integrated agent architecture for software defined radio[D]. *Sweden: Royal Institute of Telchnology*, 2000.

[2] Simon Haykin. Cognitive radio: brain-empowered wireless communications[J]. *IEEE Journal on Selected Areas in Communications*, 2005, 23(2): 201 - 220.

[3] 周贤伟,辛晓瑜,王丽娜,等. 认知无线电安全关键技术研究[J]. 电信科学, 2008, 24(2): 72 - 77.

[4] Hamdi K, Zhang W, Letaief K B. Low-complexity antenna selection and user scheduling in cognitive MIMO broadcast systems[C]// *IEEE International Conference on Communications*, 2008: 4038 - 4042.

[5] Xu hua, Xu Chengqi. Optimization of irregular LDPC codes on Rician channel[C]// *International Conference of Wireless Communications, Networking and Mobile Computing*, 2005, 1: 381 - 383.

[6] Fossorier M. Quasi cyclic low-density parity-check codes from circulant permutation matrices[J]. *IEEE Trans. on Information Theory*, 2004, 50(8): 1788 - 1793.

[7] Tanner R M, Sridhara D, Sridharan A. LDPC block and convolutional codes based on circulant matrices[J]. *IEEE Trans. on Information Theory*, 2004, 50(12): 2966 - 2984.

[8] Zhao Y, Xiao Y. A design of orthogonal interleavers for multimodes tubo en-decoders[C]// *Proc. of IEEE International Symposium on Circuits and Systems*, 2005: 3171 - 3174.

[9] Chen J H, Dholakia A, Evangelos E. Reduced-complexity decoding of LDPC codes[J]. *IEEE Trans. on Communications*, 2005, 53(8): 1288 - 1299.

[10] Li Zongwang, Chen Lei, Zeng Lingqi, et al. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. *IEEE Trans. on Communications*, 2006, 54(1): 71 - 81.

[11] 姜明,赵春明,何善宝,等. 低复杂度的 LDPC 码联合编译码构造方法研究[J]. 通信学报, 2005, 26(2): 80 - 86.

[12] 付卫红,杨小牛,刘乃安,等. 宽带无线通信中的 MIMO 系统[J]. 电子科技大学学报, 2007, 36(2): 176 - 178.

[13] 雷维嘉,谢显中,李广军. 一种基于 LDPC 编码的协作通信方式[J]. 电子学报, 2007, 35(4): 712 - 715.