融入LDPC纠错机制的认知无线电物理层认证分析

周雪倩 吴晓富 余训健
(南京邮电大学通信与信息工程学院 南京 210003)

摘 要 从信道纠错编码的角度来探讨认知无线电寄生认证信道的容量。首先,通过推导认证信道的对数似然比,给出了其简化计算方式,分析与仿真结果表明:简化计算与严格计算结果相仿,因而认证信道可等效为二元输入的加性高斯白噪声(BI-AWGN)信道。其次,基于对数似然比的简化形式,通过置信度传播迭代译码,考察了融入LDPC纠错机制的认证信道实际传输性能,仿真结果表明:实际简化译码的结果与理想BI-AWGN的译码性能无法区分。最终得出研究结论:认知无线电寄生认证信道可严格等效为BI-AWGN信道,因而可采用BI-AWGN信道设计的纠错编码来有效逼近寄生认证信道的传输极限。

关键词 认知无线电,寄生认证信道,对数似然比,二元输入加性白噪声信道,纠错编码
中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.016

LDPC Coded Primary Transmitter Authentication Schemes in Cognitive Radio Networks

ZHOU Xue-qian WU Xiao-fu YU Xun-jian
(College of Telecommunication & Information Engineering, Nanjing University of Posts and Telecommunication, Nanjing 210003, China)

Abstract In this paper, the capacity of embedded primary transmitter authentication channel in cognitive radio is investigated. By employing the log-likelihood ratios(LLRs) of a tag bit and its approximation, we showed that the equivalent authentication channel observed by the secondary receiver can be viewed as a binary-input additive white Gaussian noise (BI-AWGN) channel. Then, we investigated the practical performance of the embedded authentication channel with the use of LDPC coding. With the approximate form of LLRs, we found that it performs very close to that of belief propagation decoding over the ideal BI-AWGN channel. Hence, we concluded that a good error-control coding scheme for a BI-AWGN channel is also good for embedded primary transmitter authentication channel, and the proposed approximate form of LLRs can be well exploited to facilitate the computation in practice with low complexity.

Keywords Cognitive radio, Embedded authentication channel, Log-likelihood ratios(LLRs), Binary-input additive white Gaussian noise(BI-AWGN) channel, Error-control coding

认知无线电的提出是为了解决无线频谱资源不足的问题,但现有的频谱政策不可能开放所有的频段,认知无线电的频谱使用需要以下几个前提条件[1]。

(1)主用户(Primary user):主用户是指在现有频谱政策下被授予频段使用权的用户。他们对特定的频段具有专属使用权,其他用户不可以干扰其正常使用。

(2)次用户(Secondary user):次用户是指工作于认知无线电状态下的、未授予专属频段的、能够工作于其他未指定频段的用户。次用户在使用未授权频段时,需要时刻监测周围频谱情况,当出现主用户时,需要进行退避。

(3)主用户在使用授权频段时具有优先使用权,但工作于未授权频段时,属于次用户。

(4)所有用户均只能工作于某些频段下,不能工作在全频段下。

(5)未来频谱政策必须对次用户工作频段做出限定,需要划分专门的频段以供使用,防止因次用户工作频率在全频段上的移动造成对军事、救援、卫星等通信频段的干扰。

由于以上因素,主用户身份识别在认知无线电技术中非常关键。认知用户在通信过程中感知到主用户存在时,立即退出该信道防止对主用户产生干扰。攻击者利用这一特点,当它检测到一个空闲的频段时,就会发送模仿主用户信号特征的信号,阻止其他认知用户竞争此频段[2-3]。

现有认知无线电系统中使用能量检测建立用户身份鉴别模型。在该模型中,一个认知用户能够识别其他认知用户的信号,把非认知用户的信号均视为主用户信号。即当认知用户检测到一个它所能识别的信号时,将此信号假设为来自另一个认知用户。反之,该认知用户将认为所检测到的信号来自主用户。在这种模型中,一个自私的认知用户(一个攻击者)很容易侵入频谱感知过程,占有信道。例如,攻击者能够通过在授权频段上发送认知用户无法识别的信号达到冒充主

到稿日期:2016-05-08 返修日期:2016-08-30 本文受国家自然科学基金(61372123)资助。
周雪倩(1992—),女,硕士生,主要研究方向为无线数据与移动计算,E-mail:z_xueq@163.com;**吴晓富**(1975—),男,博士,教授,主要研究方向为编码与信息论、计算复杂性与密码学、移动计算、生物特征安全识别、无线通信与深空通信、导航信号处理等,E-mail:xfuwu@njupt.edu.cn;**余训健**(1992—),男,硕士生,主要研究方向为无线数据与移动计算,E-mail:yu_xunjian@163.com。

用户阻止其他认知用户接入这个频带的目的。甚至诸多的无恶意干扰也会占有频谱，而被认为是主用户信号。

虽然认知无线电技术促进了通信产业的快速发展，为人们的生活带来了极大的便利，但由于认知无线网络构建于现有无线网络的基础上，因此现有无线网络面临的安全问题在未来认知无线网络中同样会面临，通信安全、用户身份认证问题仍然是需要关注的重点。而物理层认证是认知无线电的安全基础，它利用物理层信号的特性来识别身份，保证通信双方是其所声称的身份，防止非法用户的接入与访问[5-12]。

1 认证标签的产生与传递

(1)认证标签的生成

认证标签是通过一条单向的 hash 链产生的：

$h_{n+1}\rightarrow h_n\rightarrow\cdots\rightarrow h_1\rightarrow h_0$

其中，$h_i=hash(h_{i+1})$。

这条 hash 链的末端 h_0 是提前告知所有接收机的。链上的每个数字只有在特定的时间区间内发送才是有效的。由于 hash 链是单向的，因此当 $j>i$ 时，由 h_i 是无法推出 h_j 的，h_i 必须在 h_j 之前发送。为了避免接收机受到不定时调谐的影响，认证标签在特定时间区间内重复发送，如图 1 所示。

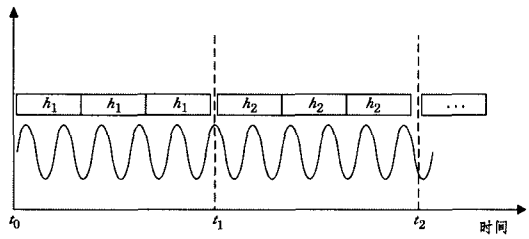


图 1 认证标签

接收机接收到信号后分离出认证标签 h_i，通过时间和已知的 h_0 对接收到的 h_i 进行认证。在认证过程中，只要 hash 链中一个数字出错，则整个认证过程都会失败，从而证明这种生成方法的安全性能是很高的。

(2)认证标签的传递

本文采用调制方式嵌入认证标签[7-8]，再通过接收机对其识别分离，这些微扰信号相当于信道中的加性噪声，并不会对信息的传递造成很大的影响，满足认证标签对信息透明的要求。

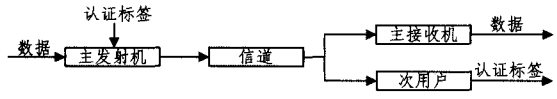


图 2 信道模型

结合文献[7]的思想，本文将认证标签看作一个微小的角度偏移 θ 加入到调制信号中进行传输。以 QPSK 为例，11，01，00，10 这 4 种信号对应 $\frac{\pi}{4}$，$\frac{3\pi}{4}$，$\frac{5\pi}{4}$，$\frac{7\pi}{4}$ 4 个相位点，经过信道的传递，信道噪声对信号产生干扰，使得星座点产生一定程度的相位偏移，因此接收机对信号进行判决时不是根据具体点的位置，而是划定了 4 个判决区域来判定 11，01，00，10 这 4 种信号。本文利用了种判决特性，设计了通过调制的方式在信号中加上认证标签，如图 3 所示。

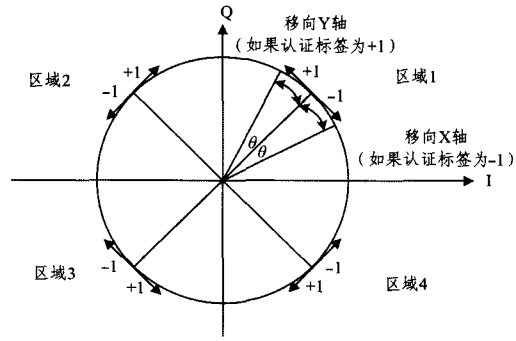


图 3 QPSK 星座图中嵌入二进制认证标签

当标签值为 1 时，将星座点向 Y 轴偏移一个微小的角度 θ；当标签值为 0 时，将星座点向 X 轴偏移一个微小的角度 θ[7]。角度 θ 值的大小有限，不会影响接收机对信号的判决。当接收机接收到信号后，根据星座点的偏移方向，划分 4 块区域来判决认证标签的值，如图 4 所示。

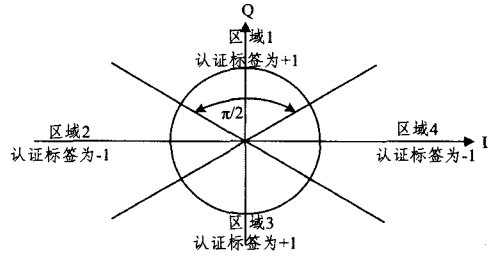


图 4 认证标签判决域

根据图 4，如果星座点落入区域 1 和区域 3，则判决标签值为 1，反之则判其为 0。

加入角度偏移 θ 后，QPSK 信号的基带等效模型为：

$$y_k=A\cdot(i_k+jq_k)\cdot e^{jg_k\cdot\theta}+w_k \tag{1}$$

其中，i_k，q_k 为 QPSK 信号的两路正交信号，i_k，$q_k\in\{+1,-1\}$；A 为信号幅度；g_k 为认证标签，$g_k\in\{+1,-1\}$；w_k 为复合高斯白噪声信号。

经过硬判决，主信号与认证标签的误码率仿真曲线如文献[7]中图 6 所示。

2 认证标签 LLR 的严格推导

本文主信号采用 QPSK 调制信号：$s_k=i_k+jq_k$，将其置于单位圆，即有：$s_k\in\{e^{j\frac{\pi}{4}},e^{-j\frac{\pi}{4}},e^{j\frac{3\pi}{4}},e^{-j\frac{3\pi}{4}}\}=\Xi,k=1,2,\cdots,N$。

认证标签为 g_k，根据图 4，如果 $g_k=+1$，QPSK 星座点即往 Y 轴方向偏移微小的角度 θ；如果 $g_k=-1$，即往 X 轴方向偏移角度 θ。当 QPSK 信号位于二、四象限时，需要对角度偏移量 θ 的正负进行翻转设置，因此接收信号的相位变化与 s_k，g_k 都有关系。

则在接收端，接收信号：

$$y_k=A\cdot s_k\cdot e^{jg_k\cdot u(s_k)\theta}+w_k,k=1,2,\cdots,N \tag{2}$$

其中：

$$u_k=\begin{cases}+1, & s_k\in\{e^{j\frac{\pi}{4}},e^{-j\frac{3\pi}{4}}\}\\ -1, & s_k\in\{e^{-j\frac{\pi}{4}},e^{j\frac{3\pi}{4}}\}\end{cases} \tag{3}$$

其中，w_k 是复合高斯噪声，$w_k=w_k^i+jw_k^q$，w_k^i 与 w_k^q 服从均值为 0、方差为 σ^2 的高斯分布。$E[(w_k)^2]=2\sigma^2$。

则认证信道的对数似然比为：

$$L_k=\log\frac{p(y_k|g_k=+1)}{p(y_k|g_k=-1)}=\log\frac{\sum_{s_k\in\Xi}p(y_k,s_k|g_k=+1)}{\sum_{s_k\in\Xi}p(y_k,s_k|g_k=-1)}=\log\frac{\sum_{s_k\in\Xi}p(y_k|g_k=+1,s_k)p_r(i_k,q_k)}{\sum_{s_k\in\Xi}p(y_k|g_k=-1,s_k)p_r(i_k,q_k)}=\log\frac{\sum_{s_k\in\Xi}p(y_k|g_k=+1,s_k)}{\sum_{s_k\in\Xi}p(y_k|g_k=-1,s_k)} \tag{4}$$

其中：

$$p(y_k|g_k=+1,s_k)\propto\exp\{\frac{-|y_k-As_k e^{jg_k\cdot u(s_k)\theta}|^2}{2\sigma^2}\}$$

$$=\exp\{0.5\cdot\frac{2A}{\sigma^2}\cdot\Re[y_k^* s_k e^{jg_k\cdot u(s_k)\theta}]\} \tag{5}$$

根据式(4)和式(5)，以及判定法则：$L_k>0, g_k=+1$，$L_k<0, g_k=-1$，画出不同信噪比下认证标签的误码率与角度偏移量 θ 之间的关系图，如图 5 所示。

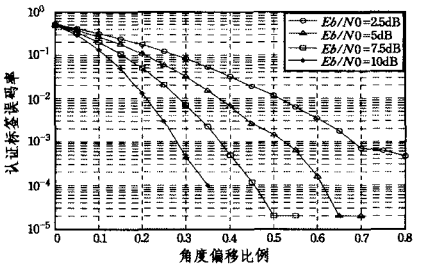
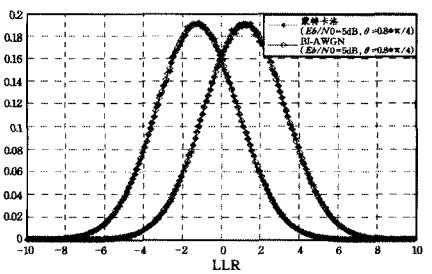


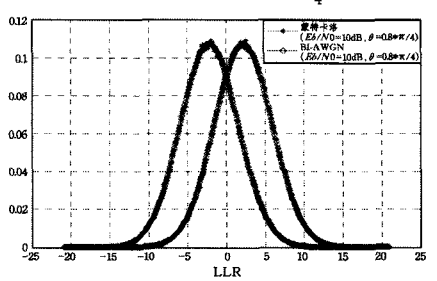
图 5　不同信噪比下认证标签的误码率曲线

如图 5 所示，当信噪比固定时，随着角度偏移量 θ 的增大，认证标签的误码率逐渐降低；在同样的角度偏移量 θ 下，信噪比越大，认证标签的误码率越低。上述结果与文献[7]中理论结果一致。

为观察等效信道的信道模型，图 6 给出了 LLR 的概率密度函数的蒙特卡洛仿真曲线。此外，还统计出 LLR 的均值和方差，并给出相应的高斯分布曲线进行对比。



(a) $Eb/N0=5\text{dB}, \theta=0.8*\frac{\pi}{4}$



(b) $Eb/N0=10\text{dB}, \theta=0.8*\frac{\pi}{4}$

图 6　严格形式下 LLR 的概率密度函数与高斯分布概率密度函数

由图 6 可以发现两条曲线基本重合，认为认证信道可以等效为二进制对称输入高斯信道(BI-AWGN)。图中左边曲线是当 $g_k=-1$ 时 LLR 的概率密度函数；右边曲线是当 $g_k=+1$ 时 LLR 的概率密度函数。由图 6 可知，寄生认证信道可等效为二元输入的加性高斯白噪声(BI-AWGN) 信道。

3　简化 LLR 推导

LLR 原始公式计算复杂，很难实现。为此，提出了一种 LLR 计算的简化算法。假定 θ 在发射和接收端是预先协商好的，且 θ 足够小，当发射信号 s_k 的星座落在某一象限，认为接收到的信号 y_k 也位于该象限。下面首先证明该假设成立：已知 s_k 位于第一象限，而 y_k 位于其他 3 个象限的概率。由于接收信号 $y_k=A\cdot s_k\cdot e^{jg_k\cdot u(s_k)\theta}+w_k$，令 $x_k=A\cdot s_k\cdot e^{jg_k\cdot u(s_k)\theta}$，将 x_k 分解成 i 和 q 两路：

$$x_k^i=\frac{A}{\sqrt{2}}[\cos(g_k\theta)-\sin(g_k\theta)]$$
$$x_k^q=\frac{A}{\sqrt{2}}[\cos(g_k\theta)+\sin(g_k\theta)] \tag{6}$$

则接收信号 y_k 位于其他象限的概率为：

$$p_{error}=p(y_k\notin Q1|x_k\in Q1)=1-p(y_k\in Q1|x_k\in Q1)=1-p(w_k^i>-x_k^i)\cdot p(w_k^q>-x_k^q)=\frac{1}{2}erfc(\frac{x_k^i}{\sigma})+\frac{1}{2}erfc(\frac{x_k^q}{\sigma}) \tag{7}$$

其中，$Q1$ 为第一象限，$erfc(x)=\frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt$。

p_{error} 随信噪比变化的仿真曲线如图 7 所示。

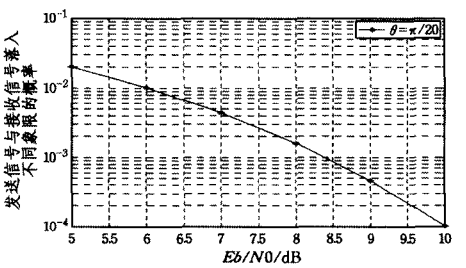


图 7　接收信号 y_k 与发送信号 s_k 不在同一象限的概率

由图 7 可知，当 θ 非常小时，可以认为发射信号 s_k 落在某一象限，接收到的 y_k 的星座的也位于该象限。

如果 y_k 落在第 I 象限，显然有：

$$|y_k-A\cdot\sqrt{2}e^{j\frac{\pi}{4}}\cdot e^{jg_k\theta}|^2<|y_k-A\cdot\sqrt{2}s_k\cdot e^{jg_k\theta}|^2$$
$$\forall s_k\in\Xi/\{e^{j\frac{\pi}{4}}\} \tag{8}$$

因此，利用 max-log-map 近似算法：

$$\exp(-|a|)+\exp(-|b|)\approx\exp(-\min\{|a|,|b|\}) \tag{9}$$

容易得到：

$$L_k\approx-\frac{1}{2\sigma^2}\{|y_k-As_k\cdot e^{j(+1)\theta}|^2-|y_k-As_k\cdot e^{j(-1)\theta}|^2\}$$
$$=\{2\Re[y_k^* Ae^{j(\frac{\pi}{4}+\theta)}-2\Re[y_k^* Ae^{j(\frac{\pi}{4}-\theta)}]\}$$
$$=\frac{2A}{\sigma^2}\sin\theta\cdot\Re[jy_k^* e^{j\frac{\pi}{4}}]$$

$$=\frac{2A}{\sigma^2}\sin\theta(y_k^Q-y_k^I) \tag{10}$$

其中，$y_k=y_k^I+jy_k^Q$。

同理可得 L_k 落在 II，III，IV 象限时的近似值：

$$\text{II}:L_k\approx-\frac{2A}{\sigma^2}\sin\theta(y_k^I+y_k^Q)$$

$$\text{III}:L_k\approx\frac{2A}{\sigma^2}\sin\theta(y_k^I-y_k^Q)$$

$$\text{IV}:L_k\approx\frac{2A}{\sigma^2}\sin\theta(y_k^I+y_k^Q)$$

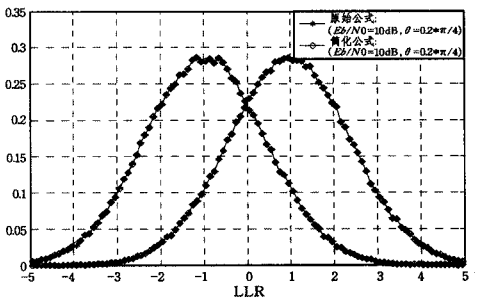
引入一个符号函数 sgn(x)：

$$\text{sgn}(x)=\begin{cases}+1, & x>0\\ 0, & x=0\\ -1, & x<0\end{cases} \tag{11}$$

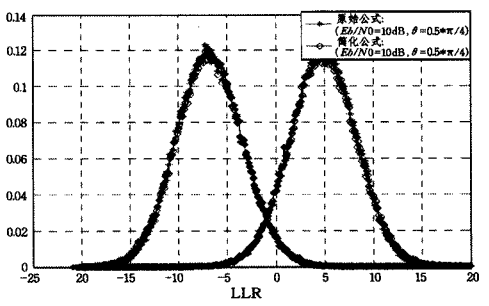
可以将 L_k 统一写成：

$$L_k\approx\frac{\sqrt{2}A}{\sigma^2}\sin\theta\left[-\text{sgn}(y_k^I)y_k^I+\text{sgn}(y_k^Q)y_k^Q\right] \tag{12}$$

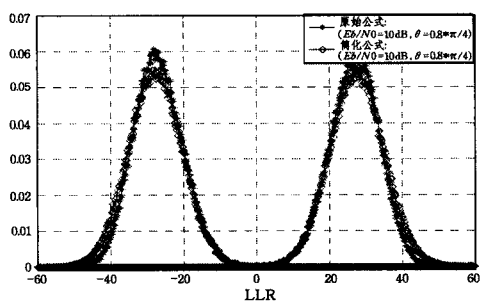
由式(12)绘出 LLR 简化公式的概率密度分布，与原始公式的曲线对比如图 8 和图 9 所示。



(a) $Eb/N0=10\text{dB},\theta=0.2*\frac{\pi}{4}$

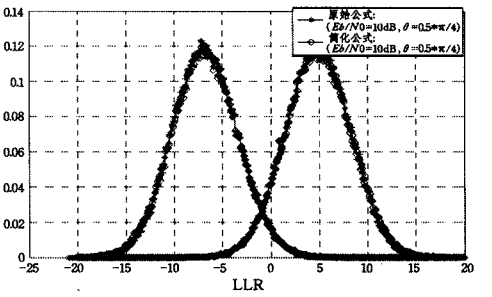


(b) $Eb/N0=10\text{dB},\theta=0.5*\frac{\pi}{4}$

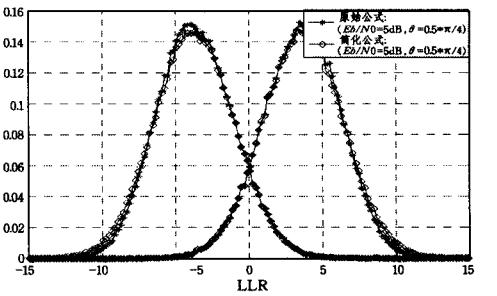


(c) $Eb/N0=10\text{dB},\theta=0.8*\frac{\pi}{4}$

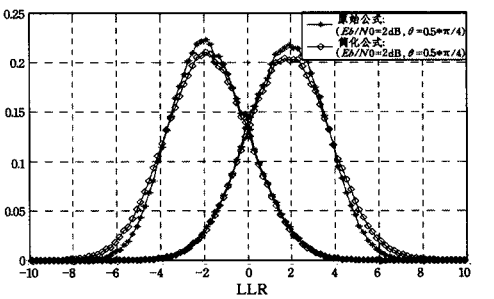
图 8 相同的 $Eb/N0$，不同的 θ 下 LLR 原始公式与简化公式概率密度函数



(a) $Eb/N0=10\text{dB},\theta=0.5*\frac{\pi}{4}$



(b) $Eb/N0=5\text{dB},\theta=0.5*\frac{\pi}{4}$



(c) $Eb/N0=2\text{dB},\theta=0.5*\frac{\pi}{4}$

图 9 相同的 θ，不同的 $Eb/N0$ 下 LLR 原始公式与简化公式概率密度函数

由图 8、图 9 可知：由简化公式与原始公式所绘出的 LLR 概率密度曲线基本重合，认证信道可等效为二元输入的加性高斯白噪声(BI-AWGN)信道，简化算法大大降低了计算复杂度。

4 等效信噪比计算

根据上述分析，$L_k\approx\frac{\sqrt{2}A}{\sigma^2}\sin\theta[-\text{sgn}(y_k^I)y_k^I+\text{sgn}(y_k^Q)y_k^Q]$，由于 $\text{sgn}(y_k^I)+j\text{sgn}(y_k^Q)=\sqrt{2}s_k$，因此可将公式化简为：

$$L_k\approx\frac{2A}{\sigma^2}\sin^2\theta\cdot g_k+\frac{\sqrt{2}A}{\sigma^2}\sin\theta(w_k^Q-w_k^I) \tag{13}$$

由式(13)进一步说明认证信道实质就是一个 BI-AWGN 信道，认证信道等效信噪比可以表示成：

$$\frac{E_s}{N_0}|_t=\frac{1}{2}\frac{(\frac{2A}{\sigma^2}\sin^2\theta)^2}{(\frac{\sqrt{2}A}{\sigma^2}\sin\theta)^2\cdot 2\sigma^2}=\frac{A^2}{2\sigma^2}\sin^2\theta \tag{14}$$

又 $\frac{E_b}{N_0}|_m=\frac{A^2}{4\sigma^2}$，因此：

$$\frac{E_b}{N_0}|_t=2\frac{E_b}{N_0}|_m\cdot\sin^2\theta \tag{15}$$

进一步可以得到：

$$\frac{E_b}{N_0}|_t = 2 \cdot R_c \sin^2\theta \cdot \frac{E_b}{N_0}|_m \tag{16}$$

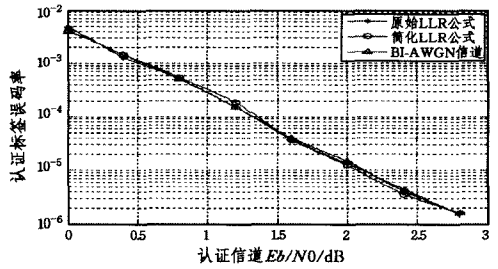
其中，$\frac{E_b}{N_0}|_t$ 表示认证信号的信噪比，$\frac{E_b}{N_0}|_m$ 表示主信号的信噪比，R_c 表示码率，每符号认证标签与每比特主信号相比有 $10\log_{10}(2\sin^2\theta)$dB 的噪比损失。

5　融入 LDPC 纠错编码机制

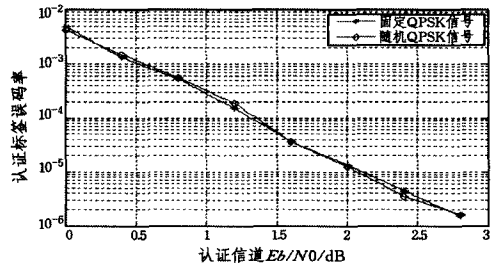
文献[8]提出采用经典的 BCH 编码和硬判决认证信道的覆盖范围将远小于主信号的覆盖范围。下面考虑将 LDPC 纠错编码机制引入认证信道中，以解决由于两种信道信道容量不匹配造成的认证信道的覆盖范围限制[3,8]。

根据等效信噪比的分析，利用 1/2 码率(256，128)的 LDPC 纠错编码对认证标签进行编译码并分析其误码率性能。

由图 10 可知，利用 LLR 原始公式和简化算法得到的认证标签经过 LDPC 编译码后的误码率曲线均与理想 BI-AWGN 信道的误码性能一致，无法区分，进一步证明了认证信道严格等效于 BI-AWGN 信道。为此，可采用 BI-AWGN 信道设计的纠错编码来有效逼近寄生认证信道的传输极限。



(a)QPSK 信号随机



(b)固定 QPSK 信号

图 10　认证标签经过 LDPC 译码后的误码率

结束语　本文从对数似然比等效信道的角度出发，首先分析了认证信道的容量，理论推导出了认知无线电寄生认证信道对数似然比的一种简化计算方法。该算法主要适用于迭代解码环境，如 LDPC/Turbo 码等，大大降低了计算的复杂度。分析与仿真表明：简化计算与严格计算结果相仿，因而认证信道可等效为二元输入的加性高斯白噪声(BI-AWGN)信道。其次研究了融入 LDPC 纠错机制的认证信道的实际传输性能，发现采用等效简化 LLR 迭代译码的结果与理想 BI-AWGN 的译码性能无法区分，由此得到以下重要结论：认知无线电寄生认证信道可严格等效为 BI-AWGN 信道，因而可采用 BI-AWGN 信道设计的纠错编码来有效逼近寄生认证信道的传输极限。

参 考 文 献

[1] STOTAS S, NALLANATHAN A. Enhancing the Capacity of Spectrum Sharing Cognitive Radio Networks [J]. IEEE Transactions on Vehicular Technology, 2011, 60(8): 3768-3779.

[2] ZHAO C D, XIE L, JIANG X Y, et al. A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks[C]// 2010 International Conference on Communications and Mobile Computing (CMC). 2010: 154-158.

[3] SHU Z H, QIAN Y, CI S. On physical layer security for cognitive radio networks [J]. IEEE Network, 2013, 27(3): 28-33.

[4] SHANNON C E. Probability of error for optimal codes in a Gaussian channel [J]. Bell System Technical Journal, 1959, 38 (3): 611-656.

[5] ZOU Y L, WANG X B, SHEN W M. Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks [J]. IEEE Transactions on Communications, 2013, 61 (12): 5103-5113.

[6] SAKRAN H, SHOKAIR M, NASR O, et al. Proposed relay selection scheme for physical layer security in cognitive radio networks [J]. IET Communications, 2012, 6(16): 2676-2687.

[7] TAN X, BORLE K, DU W, et al. Cryptographic link signatures for spectrum usage authentication in cognitive radio [C]// Proc. 2011 ACM WiSec. 2011: 79-90.

[8] JIANG T, ZENG H, YAN Q, et al. On the limitation of embedding cryptographic signature for primary transmitter authentication [J]. IEEE Wireless Communication Letter, 2012, 1(4): 324-327.

[9] BORLE K M, CHEN B, DU W K. Physical Layer Spectrum Usage Authentication in Cognitive Radio: Analysis and Implementation [J]. IEEE Transaction Inference Forensics Security, 2015, 10(10): 2225-2235.

[10] IDA A, FUJII T. Physical layer security using multi-band transmission considering channel selection for cognitive radio networks [C]// Signal and Information Processing Association, Annual Summit and Conference(APSIPA). 2014: 1-5.

[11] ZOU Y L, ZHU J, YANG L Q, et al. Securing physical-layer communications for cognitive radio networks [J]. IEEE Communications, 2015, 53(9): 48-54.

[12] CEPHELI O, KURT G K. Physical layer security in cognitive radio networks: A beamforming approach [C]// First International Black Sea Conference Communications and Networking (BlackSeaCom). 2013: 233-237.