# 利用信道衰落幅度差异隐藏私密信息的物理层安全编码方法

白慧卿 金 梁 钟 州 黄开枝
(国家数字交换系统工程技术研究中心，河南郑州 450002)

**摘 要**：针对现有物理层安全编码方法对信道差异利用不充分导致安全间隙较大的问题，本文首先建立了衰落信道下的物理层安全传输模型；然后通过分析不同衰落幅度下私密信息的译码错误概率，给出了与信道衰落幅度特征相匹配的私密信息隐藏位置选取规则；最后结合私密信息置乱将译码残余比特错误扩散到整个码字中，进一步提高窃听者对私密信息的译码错误概率。仿真结果表明，该方法的安全间隙比直接传输和仅私密信息置乱的方法分别缩小了 23.5dB 和 4.5dB。

**关键词**：物理层安全编码；信道差异；衰落幅度；低密度奇偶校验码；安全间隙；私密信息置乱
**中图分类号**：TN918 **文献标识码**：A **文章编号**：1003-0530(2015)01-0017-09

# The Physical Layer Secrecy Coding Method of Hiding Confidential Information using Amplitude Difference of Fading Channel

BAI Hui-qing JIN Liang ZHONG Zhou HUANG Kai-zhi
(National Digital Switching System Engineering & Technological Research Center, Zhengzhou, Henan 450002, China)

**Abstract**: This paper focused on the problem that the existing physical layer secrecy coding has a large security gap caused by the insufficient using of channel characteristic difference. Firstly, this study established a physical layer secrecy transmission model in fading channel. Then through the analysis of the bit error probability of confidential information under different channel fading amplitude, a channel fading amplitude matched confidential information hiding place selection rule is given. Finally the scrambling was used to spread the error to the whole code words, which increased Eve's error probability. The simulation results show that the security gap of this method is reduced by 23.5dB and 4.5dB compared with direct transfer and scrambling, respectively.

**Key words**: physical layer secrecy coding; channel difference; fading amplitude; low-density parity-check codes; security gap; confidential bits scrambling

## 1 引言

1975 年 Wyner 等人提出的窃听信道模型[1]，指出通过合适的编码可以达到通信的保密容量，实现无密钥条件下的安全传输，即编码的“一次一密”[2]，物理层安全编码由此诞生。物理层安全编码在保证授权节点间信息传输可靠性的同时，能够利用无线信道天然的差异性与通信双方信道特征的互易性使窃听者无法获取任何私密信息，是物理层安全的重要技术之一。其本质是一种加入了安全约束的特殊信道编码，不依赖于窃听者计算能力限制实现安全通信，具有重要的现实意义和广阔的应用前景。

无线信道的差异性是物理层安全的实现基础，

收稿日期：2014-03-20；修回日期：2014-09-05
基金项目：国家自然科学基金资助课题（61171108）

目前,众多学者围绕如何利用无线信道差异进行安全编码方法设计展开研究。Jiaxi Xiao 等人提出随机复数域编码[3],将私密信息淹没在随机数据中,从而确保信息安全传输,然而其结果基于合法信道无噪的假设。文献[4]-[10]的工作在合法信道有噪的条件下展开:JaeKwak 提出的反格雷星座映射编码[4],通过缩小相邻码字在星座图上的欧氏距离,提升低信噪比下的误码率;王亚东等人针对多天线系统提出了一种基于信道特征随机投影的物理层安全编码方式[5],能够使合法接收端的码字极性恒定,而窃听者接收码字的极性正负交替;Klinc 提出了一种打孔低密度奇偶校验(low-density parity-check, LDPC)码[6-7],将私密信息隐藏在打孔位中不直接传输,利用接收到得其余信息译码恢复私密信息,达到安全传输的目的,并以最小化安全间隙为目标研究最优的打孔分布;Baldi 将私密信息置乱与信道编码相结合,通过在信道编码前级联一个非奇异随机置乱矩阵 $\mathbf{S}$,将信道译码后的残余错误扩散到全部符号中,并指出当 $\mathbf{S}^{-1}$ 的密度近似0.5时这种错误扩散效果最为明显[8-10]。

上述安全编码方法大多是在 AWGN 信道下基于信道编码码字结构进行设计的,利用了信道噪声增加窃听者的接收信息疑义度,确保需要安全传输的私密信息在窃听信道中被噪声淹没,最终达到信息安全的效果。然而,在无线通信中,不同信道的差异性不仅体现为噪声功率不同,其还体现在信道的幅度、相位等特征[11]的差异上,仅利用信道噪声差异从码字结构角度进行安全编码设计,获得的安全增益有限。

受 Klinc 等人的启发,本文在瑞利衰落信道模型下,将信道衰落幅度特征与 LDPC 编码相结合,利用合法信道与窃听信道间衰落幅度图样的差异,在编码码字中合理选取私密信息的隐藏位置,构造有利于合法接收者可靠接收的条件,提出了一种利用信道衰落幅度差异隐藏私密信息的物理层安全编码方法。该方法首先对 LDPC 码中不同信道衰落幅度上信息节点的译码错误概率进行分析,证明在信道能量相同的条件下隐藏节点所对应的信道衰落幅度越小越有利于该节点处的信息正确恢复。利用这一特性,发送端通过信道估计获得合法信道的衰落幅度图样,根据该图样选取衰落幅度最小的位置作为私密信息的隐藏位,形成合法接收者译码性能占优的条件,再通过信息置乱对译码残余错误形成扩散,进一步缩小安全间隙,实现物理层安全传输。

## 2 物理层安全传输模型与安全性评价

合法信道质量优于窃听信道质量是保密容量存在的前提,同时也是实现物理层安全编码的必要条件。当天然信道不满足合法信道质量占优的条件时,常采用人工噪声[12-13]、跳空[14-15]等物理层安全技术通过在发射端发送人工干扰或随机选择空域信道来破坏窃听者的接收性能,降低窃听信道的可达信道容量,为安全编码创造信道条件优势。若发射端的人工噪声波束赋形矢量或跳空图样随符号变化时,则可以等效为发送信号经过了一个快衰落信道到达接收端,因此,本节建立了瑞利衰落信道下的物理层安全传输模型,并在此模型基础上展开与信道衰落幅度相匹配的安全编码技术研究。

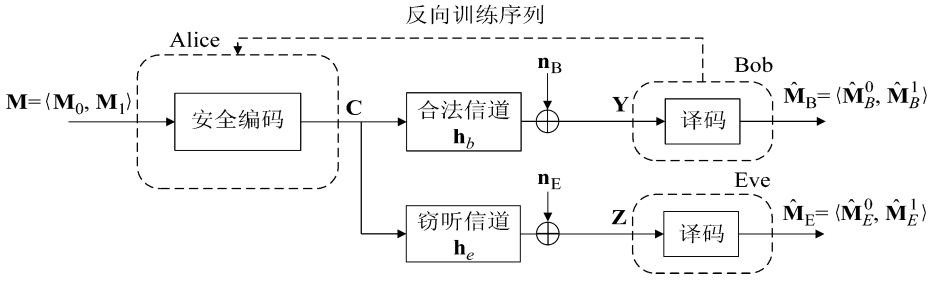



图1 物理层安全传输模型

Fig. 1 The physical layer secrecy transmission model

如图 1 所示,发送者 Alice 将长度为 $k$ 的原始信息符号 $\mathbf{M}$ 进行安全编码,得到长为 $N$ 的待发送符号 $\mathbf{C}$,其中 $\mathbf{M}$ 分别由长度为 $s$ 的私密信息 $\mathbf{M}_0$ 和长度为($K$-$s$)的公共信息 $\mathbf{M}_1$ 组成,且 $\mathbf{M}_0$ 与 $\mathbf{M}_1$ 相互独立。$\mathbf{C}$ 经合法信道与窃听信道传输分别到达合法接收者 Bob 与窃听者 Eve,假设合法信道与窃听信道是独立同分布的瑞利衰落信道,则 $i$ 时刻的接收信号分别表示为:

$$\begin{aligned} y(i) &= h_b(i) \cdot x(i) + n_b(i) \\ z(i) &= h_e(i) \cdot x(i) + n_e(i) \end{aligned} \tag{1}$$

其中,$x(i)$ 表示 $i$ 时刻的发送符号;$h_b(i)$ 与 $h_e(i)$ 分别表示 $i$ 时刻合法信道和窃听信道的瑞利衰落系数,其概率密度函数满足 $f(h_b(i)) = 2h_b(i) \cdot \exp(-h_b^2(i))$,$f(h_e(i)) = 2h_e(i) \cdot \exp(-h_e^2(i))$;$n_b(i)$ 和 $n_e(i)$ 分别表示合法信道和窃听信道中独立同分布的加性高斯白噪声,其均值为 0,方差分别为 $\sigma_b^2$ 和 $\sigma_e^2$。Bob 和 Eve 分别对接收到的符号 $\mathbf{Y}$、$\mathbf{Z}$ 进行译码,得到对原始信息的恢复 $\hat{\mathbf{M}}_B$、$\hat{\mathbf{M}}_E$,其中私密信息部分分别为 $\hat{\mathbf{M}}_B^0$ 和 $\hat{\mathbf{M}}_E^0$。

此时,为保证 Alice 与 Bob 间通信的可靠性及与 Eve 间的安全性,需满足条件:

$$\begin{cases} I(M_0, \hat{M}_B^0) = H(M_0), \text{(可靠性)} \\ I(M_0, \hat{M}_E^0) = 0. \text{(安全性)} \end{cases} \tag{2}$$

上式表明,Bob 获得输出符号 $\hat{M}_B^0$ 后对于输入的私密信息不存在任何不确定性,私密信息通过合法信道没有任何损失,同时,在窃听信道中私密信息与 Eve 获得的输出符号 $\hat{M}_E^0$ 间没有任何依赖关系,Eve 从接收符号中获得的关于私密信息的信息量等于零。

当 Alice 发射总功率为 $P$,码字传输时间内合法信道与窃听信道具有相同的信道能量 $E[h_b^2(i)] = E[h_e^2(i)]$ 且噪声功率 $\sigma_b^2 = \sigma_e^2 = \sigma^2$ 时,图 2 给出了一个安全编码性能衡量示意图。横轴表示发射信噪比(signal to noise ratio, SNR),即 $P/\sigma^2$,纵轴表示私密信息的误比特率(bit error rate, BER)。当 SNR≥$\mathrm{SNR}_{B,\min}$时,Bob 能够可靠接收到私密信息,即 $P_{e,\max}^B \approx 0$;当 SNR≤$\mathrm{SNR}_{E,\max}$时,Eve 几乎无法获得任何私密信息,即 $P_{e,\min}^E \approx 0.5$,安全间隙表示为 $\mathrm{SNR}_{B,\min}$ 与 $\mathrm{SNR}_{E,\max}$之差。从安全的角度来讲,需要设计一个安全间隙尽可能小的安全编码方法,减小对窃听信道 SNR 的客观要求,使得 Eve 在 SNR 略低于、甚至高于 Bob 的情况下能实现信息安全传输。

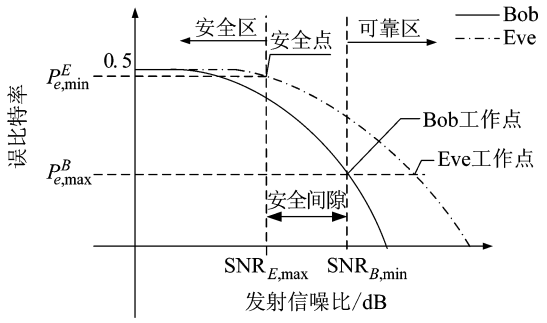



图 2　安全间隙示意图

Fig. 2　The security gap

文献[4]-[10]将信道假设为 AWGN,这样虽简化了分析,但在无形中平滑了不同接收端的信道特征差异,将编码性能与信道间的多元函数关系退化为仅与信道噪声功率有关的一元函数。然而在实际无线信道中,即使不同接收信道的噪声功率相同,信道幅度相位等特征间仍然存在差别,这就可以成为区分不同接收者的重要特征。为进一步缩小安全间隙,本文在衰落信道下,提出了一种利用信道衰落幅度差异隐藏私密信息的安全编码方法。该方法的主要思想是根据信道衰落幅度图样对私密信息 $\mathbf{M}_0$ 的比特进行重新排序,并在实际传输中采用随机比特替换 $\mathbf{M}_0$,即将 $\mathbf{M}_0$ 隐藏在发送序列中,接收端利用收到的公共信息和校验信息实现对隐藏私密信息的恢复。因此,在该安全编码方法中如何根据信道衰落幅度合理选取私密信息隐藏位置是影响其安全性能的关键,下面首先对不同衰落幅度下私密节点的译码可靠度进行分析,然后利用分析结果指导安全编码设计。

## 3　不同衰落幅度下私密信息节点的译码可靠度分析

本文选取 LDPC 码作为母码,研究缩小安全间隙的安全编码方法。一方面,安全编码的母码必须具有较强的纠错特性,LDPC 是一种性能接近 Shannon 限的信道编码,能够为私密信息的可靠传输提供保证;另一方面,LDPC 码可采用迭代消息传递(message passing, MP)译码算法,具有较小的译码复杂度,并可以通过密度进化[7]和高斯近似[6,16]等理

论工具对译码错误概率做渐进分析。

假设发送方获得完美的信道状态信息(channel state information, CSI),原始信息符号为 $M=\{m_1,m_2,\cdots,m_K\}$,LDPC 编码后信息符号为 $X=\{x_1,x_2,\cdots,x_N\}$。为便于分析,假设数据采用 BPSK 调制方式,则待发射符号为 $C=\{c_1,c_2,\cdots,c_N\}$,接收符号为 $Y=\{y_1,y_2,\cdots,y_N\}$。对于不相关瑞利衰落信道,信道输出 $y$ 的条件概率分布为:

$$f(y_i\mid c_i,h_b(i))=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(y_i-c_i\cdot h_b(i))^2}{2\sigma^2}\right)$$

其中,调制映射规则为 $C=1-2X$,$\sigma^2$ 为信道高斯白噪声功率。LDPC 码对应的校验矩阵可以用 Tanner 图表示,其中与变量节点(校验节点)相连的出边数称为变量节点(校验节点)的度,具有相同度的变量节点(校验节点)的所有出边占总边数的百分比所构成的分布函数称为变量节点(校验节点)的度分布。记 $dl$ 和 $dr$ 分别表示变量节点和校验节点度的最大值,$\nu_i(i=2,3,\cdots,dl)$ 和 $u_j(j=2,3,\cdots,dr)$ 分别表示度为 $i$ 的变量节点和度为 $j$ 的校验节点,则在对数域上的置信传播(log-likelihood ratio belief propafation, LLR-BP)译码算法中,变量节点 $\nu_i$ 向其邻居校验节点传递的初始似然比信息为:

$$L(\nu_i)=\log\frac{\Pr(c_i=1\mid y_i,h_b(i))}{\Pr(c_i=0\mid y_i,h_b(i))}=\frac{2}{\sigma^2}y_i\cdot h_b(i) \tag{3}$$

可以看出 $L(\nu_i)$ 的符号表示对变量节点的判决结果($L(\nu_i)>0$ 则 $c_i=1$,反之 $c_i=0$),幅度则表示该结果的置信概率。由于在实际传输中,私密信息被隐藏而替换为随机比特,因此接收端为避免该处的变量节点携带的初始信息对译码正确性产生负面影响,在译码初始时将该变量节点删除,即 $L(\nu_i)=0,\ i\in S$,$S$ 为全体私密信息位置的集合。

为便于算法描述,令 $\lambda_i(\rho_i)$ 表示度为 $i$ 的变量节点(校验节点)所有出边占总边的百分比,$\pi_i$ 表示对度为 $i$ 的变量节点的删除率,$p$ 表示所有删除变量节点占总节点数的百分比,则 $\lambda(x)=\sum_{i=2}^{dl}\lambda_i x^{i-1}$($\rho(x)=\sum_{i=2}^{dr}\rho_i x^{i-1}$)表示变量节点(校验节点)的度分布,$\pi(x)=\sum_{i=2}^{dl}\pi_i x^{i-1}$ 表示隐藏节点的度分布,$p=\sum_{i=2}^{dl}\frac{\lambda_i/i}{\sum_{i=2}^{dl}\lambda_i/i}\pi_i$。因此,在 BP 译码过程中,利用高斯近似对 $k$ 次迭代后变量节点的平均译码错误概率进行分析,其结果可表示为[17]:

$$\begin{aligned}P_e^{(k)}&=P_{e1}^{(k)}+P_{e2}^{(k)}\\&=\sum_{j=2}^{dl}\lambda'_j\pi_j\sum_{i=0}^{j}\mathcal{X}_{i,j}^{(k)}Q\left(\sqrt{\frac{im_u^{(k)}}{2}}\right)\\&\quad+\sum_{j=2}^{dl}\lambda'_j(1-\pi_j)\sum_{i=0}^{j}\mathcal{X}_{i,j}^{(k)}Q\left(\sqrt{\frac{im_u^{(k)}+m_\nu^{(0)}}{2}}\right)\end{aligned} \tag{4}$$

其中,$\lambda'_j=\frac{\lambda_j/j}{\sum_{i=2}^{dl}\lambda_j/j}$,$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}\mathrm{d}t$;$\mathcal{X}_{m,n}^{(k)}=C_n^m(\varepsilon^{(k-1)})^{n-m}(1-\varepsilon^{(k-1)})^m$,$\varepsilon^{(k)}$ 为度分布的函数,表示 $k$ 次迭代后删除变量节点未能恢复的概率。$m_u^{(k)}$ 表示第 $k$ 次迭代时校验节点 $u$ 向其邻居变量节点传递消息的均值,可由(5)式进行计算:

$$\begin{aligned}m_u^{(k)}&=\sum_{j=2}^{dr}\rho_j\phi^{-1}\left(1-\left[1-\sum_{i=2}^{dl}\lambda_i\phi(m_\nu^{(0)}+(i-1)m_u^{(k-1)})\right]^{(j-1)}\right)\\\phi(x)&=\begin{cases}1-\frac{1}{\sqrt{4\pi x}}\int_{\mathrm{R}}\tanh\frac{u}{2}e^{\frac{-(u-x)^2}{4x}}\mathrm{d}u, & x>0\\1, & x=0\end{cases}\end{aligned} \tag{5}$$

其中,$m_\nu^{(0)}=E[\nu\mid\nu\neq0]$ 表示非删除变量节点初始时从信道获得的对数似然比消息的均值,$\phi(x)$ 是 $[0,\infty)$ 上的连续单调减函数。

(4)式第一项表示截止到第 $k$ 次迭代,码字中的删除变量信息节点的译码错误概率;第二项表示其余信息节点上的消息译码错误概率。由于本文研究物理层信息安全传输问题,为提高窃听者对私密信息的不确定程度需要将私密信息隐藏在编码符号中,所以只关注(4)式中的第一项。已知所有删除变量节点占总节点数的百分比为 $p$,故其平均比特错误概率可以表示为:

$$P_{e,p}^{(k)}=\frac{1}{p}P_{e1}^{(k)} \tag{6}$$

可以看到,影响 $P_{e,p}^{(k)}$ 的因素除 LDPC 码的度分布参数外,还包含迭代均值 $m_u^{(k)}$($p=\sum_{i=2}^{d\nu}\lambda'_j\pi_j$ 亦是度分布

的函数)。由于对同一发送者发出的编码符号其度分布$\lambda(x)$、$\rho(x)$已定,且度分布$\pi(x)$最优时的安全编码性能与非最优相比仅提升了约0.5dB[6,7],故在此忽略度分布对 $P_{e1}^{(k)}$ 的影响,可以将 $P_{e,p}^{(k)}$ 看做关于 $m_u^{(k)}$ 的函数。由于 $Q(\cdot)$为单调减函数,若想获得较小的 $P_{e,p}^{(k)}$,需提高 $m_u^{(k)}$。

**定理 1**　给定度分布的 LDPC 码经不同信道传输,采用 LLR-BP 译码算法时,如果变量节点从信道获得的初始 LLR 消息均值满足 $m_{\nu,b}^{(0)}>m_{\nu,e}^{(0)}$,则译码迭代过程中始终有 $m_{u,b}>m_{u,e}$。

**证明**　由(5)式可得,初始 LLR 消息均值分别为 $m_{\nu,b}^{(0)}$和 $m_{\nu,e}^{(0)}$时,一次迭代后的消息均值可分别表示为:

$$m_{u,b}^{(1)}=\sum_{j=2}^{dr}\rho_j\phi^{-1}\left(1-\left[1-\sum_{i=2}^{dl}\lambda_i\phi(m_{\nu,b}^{(0)})\right]^{(j-1)}\right)$$

$$m_{u,e}^{(1)}=\sum_{j=2}^{dr}\rho_j\phi^{-1}\left(1-\left[1-\sum_{i=2}^{dl}\lambda_i\phi(m_{\nu,e}^{(0)})\right]^{(j-1)}\right)\tag{7}$$

由于 $\phi(x)$是$[0,\infty)$上的连续单调减函数,则 $\phi^{-1}(x)$为$(0,1]$上的连续单调减函数,且 $m_{\nu,b}^{(0)}>m_{\nu,e}^{(0)}$,可得 $\phi(m_{\nu,b}^{(0)})<\phi(m_{\nu,e}^{(0)})$,即 $m_{u,b}^{(1)}>m_{u,e}^{(1)}$。

假设 $m_{u,b}^{(k-1)}>m_{u,e}^{(k-1)}$ 成立,则由(5)式可得:

$$m_{u,b}^{(k)}=\sum_{j=2}^{dr}\rho_j\phi^{-1}\left(1-\left[1-\sum_{i=2}^{dl}\lambda_i\phi(m_{\nu,b}^{(0)}+(i-1)m_{u,b}^{(k-1)})\right]^{(j-1)}\right)$$

$$m_{u,e}^{(k)}=\sum_{j=2}^{dr}\rho_j\phi^{-1}\left(1-\left[1-\sum_{i=2}^{dl}\lambda_i\phi(m_{\nu,e}^{(0)}+(i-1)m_{u,e}^{(k-1)})\right]^{(j-1)}\right)\tag{8}$$

由于 $m_{\nu,b}^{(0)}>m_{\nu,e}^{(0)}$,故 $m_{u,b}^{(0)}+(i-1)m_{u,b}^{(k-1)}>m_{u,e}^{(0)}+(i-1)m_{u,e}^{(k-1)}$,所以 $m_{u,b}^{(k)}>m_{u,e}^{(k)}$成立。

由数学归纳法,当 $m_{\nu,b}^{(0)}>m_{\nu,e}^{(0)}$时,始终有 $m_{u,b}>m_{u,e}$。

证毕。

定理 1 表明若想提高节点在译码迭代过程中的消息均值 $m_u^{(k)}$,需设法增大节点的初始消息均值 $m_\nu^{(0)}$。为进一步研究信道衰落幅度与 $P_{e,p}$之间的关系,提出定理 2。

**定理 2**　给定度分布的 LDPC 码,采用 LLR-BP 译码算法时,如果在信息传输时间内合法信道的衰落幅度 $h_b(i)$与窃听信道的衰落幅度 $h_e(i)$是独立同分布的瑞利型随机变量,满足 $E[h_b^2(i)]=E[h_e^2(i)]$,$S$ 表示全体私密信息隐藏位置所构成的集合,且对 $\forall j\in S$ 有 $E[h_b(j)]<E[h_e(j)]$成立,则 $P_{e,p}^B<P_{e,p}^E$。

**证明**　由(3)式可得 Bob 和 Eve 迭代译码的初始值可分别表示为:

$$m_{\nu,b}^{(0)}=E[\nu_b\mid\nu_b\neq0]=\frac{2}{\sigma^2(1-p)n}\cdot\sum_{j\notin S}h_b^2(j)$$

$$m_{\nu,e}^{(0)}=E[\nu_e\mid\nu_e\neq0]=\frac{2}{\sigma^2(1-p)n}\cdot\sum_{j\notin S}h_e^2(j)\tag{9}$$

其中,$n$ 为变量节点总数。由于 $E[h_b^2(i)]=E[h_e^2(i)]$,则 $\sum_{j=1}^{N}h_b^2(j)=\sum_{j=1}^{N}h_e^2(j)$;当给定 LDPC 码的度分布时,删除变量节点占总节点的百分比 $p$ 一定,且对 $\forall j\in S$ 有 $E[h_b(j)]<E[h_e(j)]$成立,此时 $\sum_{j\notin S}h_b^2(j)>\sum_{j\notin S}h_e^2(j)$,因此 $m_{\nu,b}^{(0)}>m_{\nu,e}^{(0)}$。根据定理 1,可得 $m_{u,b}>m_{u,e}$。由(4)式和(6)式,$P_{e,p}$是 $m_u$ 的减函数,因此 $P_{e,p}^B<P_{e,p}^E$。

证毕。

定理 2 表明,当码字传输时间分组内的合法衰落信道与窃听信道的信道能量相同时,选取合法信道衰落幅度最小的相应位置隐藏私密信息,有利于合法接收端对私密信息的恢复,并且由于窃听信道的衰落图样不同于合法信道,即使窃听者确知相应的私密信息位置译码错误概率仍大于合法接收者。直观地讲,这是由于随机比特替换隐藏了私密信息,因此私密信息位置上的初始 LLR 消息 $L(\nu_i)=0$,对译码过程没有贡献,恢复能力仅取决于 LDPC 母码的度分布以及其余公共信息和校验信息的初始 LLR 消息,所以对于 Bob 来讲私密信息传输时刻的信道增益最小,那么其余信息传输时的信道平均增益就最大,这样就增加了接收端对译码有贡献的那部分信息的 SNR,因此提升了译码可靠性;但对 Eve 来讲,私密信息传输并非对应窃听信道衰落幅度最小的部分,其平均译码性能必然劣于 Bob。

## 4　利用信道衰落幅度差异隐藏私密信息的安全编码方法

依据第 3 节对不同衰落幅度下 LDPC 码私密信息节点的译码可靠度分析以及定理 2 的结论,本文

以信道衰落幅度图样作为区分不同接收者的重要特征,将安全编码与合法信道特征相适应,选取合法信道衰落幅度最小的位置隐藏私密信息,提高 Bob 对私密信息的译码可靠度;由于窃听信道衰落幅度图样不同于合法信道,上述位置的选取并不会提高 Eve 的接收性能,故该方法可以利用信道差异形成合法接收者对私密信息的安全可靠接收。同时,在编码前对私密信息进行信息置乱[8-10],对 Eve 译码后的残余错误进行扩散,提高低 SNR 时 Eve 的误码率,进一步提高信息传输的安全性。

图 3 给出了本文安全编码方法的结构示意图,具体共分为以下 6 个步骤:

**步骤 1** 信道估计。通信开始时,首先由 Bob 向 Alice 发射导频信号或训练序列,Alice 收到后对合法信道的衰落幅度进行估计。为不失一般性,假设 Eve 能够对这一过程实施窃听。

**步骤 2** 私密信息置乱。Alice 根据私密信息符号的长度 $s$ 随机构造一个密度为 0.5 的非奇异矩阵 $\mathbf{S}_{s\times s}$,对私密信息 $\mathbf{M}_0$ 进行置乱后得到 $\mathbf{M}'_0$,然后将 $\mathbf{M}'_0$ 与公共信息 $\mathbf{M}_1$ 按原排列重组为信息 $\mathbf{M}'$。

**步骤 3** 选取私密信息的最佳位置。Alice 根据获取的合法信道 CSI 得到信道的衰落幅度图样,选取幅度最小的 $s$ 个位置生成交织表,使得私密信息 $\mathbf{M}'_0$ 经交织后位于该最小幅度位置上,并将交织规则反馈给 Bob。为不失一般性,假设 Eve 能够对反馈过程实施窃听。

**步骤 4** 安全编码。发送端首先将 $\mathbf{M}'$ 进行系统的 LDPC 编码;然后根据步骤 3 的交织表对得到符号 $\mathbf{X}$ 进行交织,使得 $\mathbf{X}$ 中的私密信息 $\mathbf{M}'_0$ 位于合法信道衰落幅度最小的位置上;最后,在调制发射前用随机比特将相应位置的私密信息 $\mathbf{M}'_0$ 覆盖,即将私密信息隐藏在符号序列中构成待发送符号 $\mathbf{C}$,使得接收端无法直接从接收到的初始信息中获取有关私密信息的任何信息量,增加窃听者在低 SNR 下的窃听难度。

**步骤 5** 译码。接收端解调后先对接收符号进行解交织,恢复出正确的校验约束位置排列;然后采用 LLR-BP 译码算法进行译码。需要注意的是,为了防止步骤 4 中引入的随机比特对私密信息译码正确性产生负面影响,输入译码器的私密信息相应位置上的初始 LLR 消息需置零。最后,经有限次迭代译码,接收端从中恢复出置乱的私密信息。

**步骤 6** 私密信息解置乱。接收端将译码得到的私密信息矢量 $\hat{\mathbf{M}}'_0$ 与解置乱矩阵 $\mathbf{S}^{-1}$ 相乘,恢复出对原始私密信息符号的估计 $\hat{\mathbf{M}}_0$。

## 5 性能仿真与分析

本节对所提出的利用信道衰落幅度差异隐藏私密信息的安全编码方法的效果进行仿真,参照 802.16e 协议中的 LDPC 编码标准,在发端采用母码的码率 $R_K=\frac{1}{2}$,原始信息长度 $K=1152$,$N=\frac{K}{R_K}=2304$;$s=768$,则私密信息码率 $R_S=\frac{s}{n}=\frac{1}{3}$。置乱矩阵 $\mathbf{S}$ 的密度为 0.5,数据采用 BPSK 调制后经参数 $\sigma_r=\sqrt{\frac{1}{2}}$ 的瑞利衰落信道上传输,且合法信道与窃听信道衰落幅度独立同分布,两信道具有相同的高斯白噪声,噪声功率为 $\sigma^2$;取门限 $P^B_{e,\max}=10^{-6}$,$P^E_{e,\min}=0.5$,最大译码迭代次数 $k=40$。

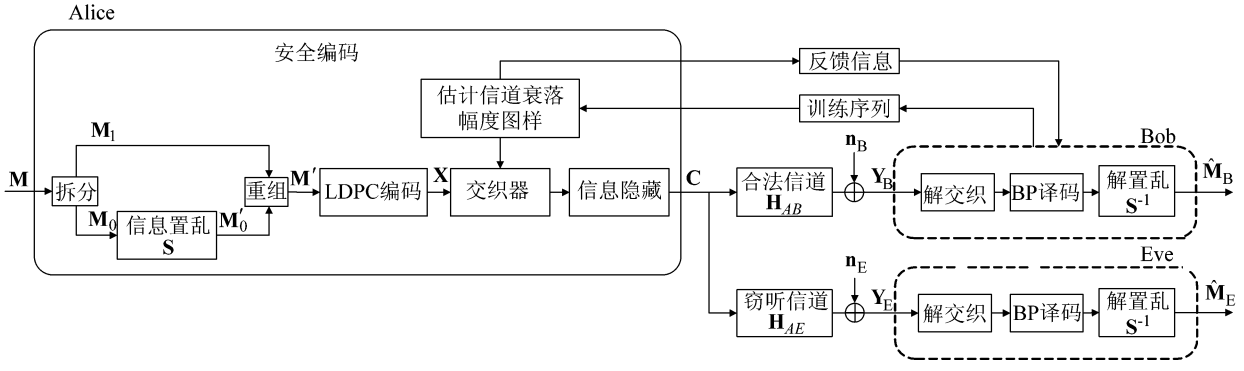



图 3 利用信道衰落幅度差异的安全编码方法结构图

Fig. 3 The diagram of secrecy coding method by using amplitude difference of fading channel

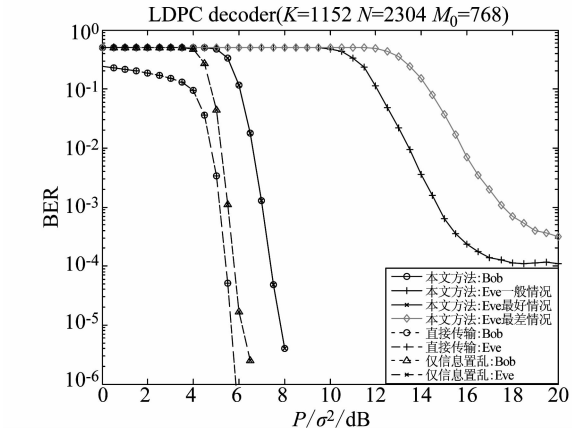



图 4　安全编码方法的误码率性能

Fig. 4　The BER performance of secrecy coding

仿真在相同发射功率、不同信道噪声功率条件下对 Alice 发出的符号进行了 $10^6$ 次独立试验,统计了 Bob 和 Eve 对私密信息的 BER,并假设 Alice 可以获得准确的 CSI 用于估计合法信道的衰落幅度图样,结果如图 4 所示。可以看到,使用本文的安全编码方法,合法用户 Bob 接收信号的 BER 随 SNR 的增加迅速降低,而窃听者 Eve 一般情况下的 BER 曲线需要更高 SNR 才能实现无误码。仿真过程中,考虑信道的时变性,每次试验均独立产生合法信道和窃听信道的衰落幅度并根据合法信道选取私密信息位,经统计 Bob 和 Eve 的 BER 曲线分别对应于图 4 中的“本文方法:Bob”和“本文方法:Eve 一般情况”,此时的安全间隙 $S_g=-1.0$dB,即窃听信道的发射 SNR 比合法信道略高,也能保证私密信息安全传输。

在本文方法的仿真中考虑了两种极端的情况:(1)若窃听信道衰落幅度图样恰好与合法信道的完全相同,此时两信道间没有瞬时衰落幅度上的差异,只有信道噪声不同,所以本文方法对 Bob 和 Eve 的影响是等价,那么 BER 退化为一条曲线(见图 4 中曲线“本文方法:Eve 最好情况”),此时的安全间隙 $S_g=4.0$dB;(2)若窃听信道衰落幅度图样恰好与合法信道的完全相反,即合法信道衰落幅度最小的部分恰好对应于窃听信道衰落幅度最大的部分,根据合法信道选取的私密信息位置对窃听者来讲最差(见图 4 中曲线“本文方法:Eve 最差情况”),此时安全间隙 $S_g=-3.0$dB。

作为对比,图 4 还给出了直接用 $R_k=\frac{1}{2}$ 的 LDPC 信道编码,以及仅将信道编码与信息置乱相结合传输私密时 Bob 和 Eve 的 BER 曲线,仿真过程中的编码信息长度、私密信息长度和随机置乱矩阵的密度均与之前描述一致。从图中可以看到,由于这两种编码方法并没有针对合法信道特征设计,Bob 的接收 SNR 不会因编码方式而改善,其与 Eve 具有相同的接收 SNR,所以两者的 BER 性能曲线重合,此时只有结合人工噪声等方法增大窃听信道噪声才能保证信息安全传输。直接采用信道编码传输时,错误码字仅来源于信道译码的残余错误,安全间隙 $S_g=22.5$dB,难以保证私密信息的安全;采用传统基于码字设计的信息置乱方法时,能够产生促进错误信息扩散的效果,相比直接传输的方法提高了 Eve 在低 SNR 下的 BER,安全间隙 $S_g$ 缩小为 3.5dB,但由于其缺乏对信道特性差异的考虑,安全间隙比本文方法大 4.5dB,私密信息的安全性劣于本文方法。

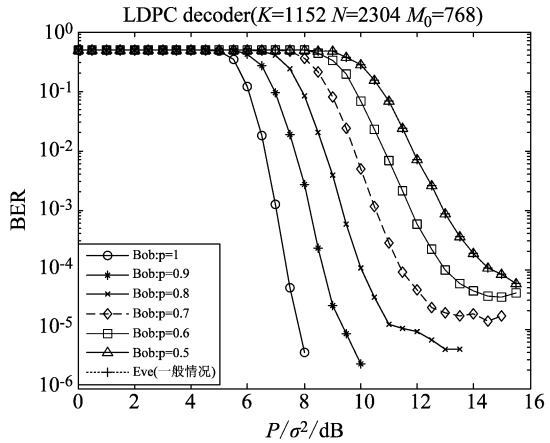



图 5　CSI 不准确时的误码率性能

Fig. 5　The BER performance of unperfect CSI

以上为 Alice 对合法信道 CSI 估计准确的情况。然而,当信道估计不准确时,Alice 会对合法信道衰落幅度的相对大小产生误判,无法准确获得衰落幅度图样,对私密信息位置的选取并非最优,进而使合法接收者的 BER 性能受到影响。假设 Alice 有能力将 $p\cdot s$ 比特私密信息随机地隐藏在幅度最小的 $s$ 个比特位置中,而误将 $(1-p)\cdot s$ 比特随机隐藏在剩余的幅度较大的位置上,其中 $0.5\leqslant p\leqslant 1$ 为私密信息百分比。仿真结果如图 5 所示,随着 $p$ 的减小,

Bob 的 BER 性能逐变差;$p=0.5$ 时,Alice 随机将私密信息隐藏在各个位置上,此时对于 Bob 来讲相当于并未从信道上获得任何编码优势,Bob 与 Eve 的 BER 重合为一条曲线,安全间隙为 10.5dB;$p=1$ 时,表示 Alice 将全部私密信息隐藏在衰落幅度最小的位置上,即完美估计 CSI,Bob 的 BER 性能最优,安全间隙为-1.0dB。

## 6 结论

本文研究了衰落信道下 LDPC 码中不同位置的信息节点译码后的错误概率,理论分析表明私密信息节点位于衰落幅度较小的位置时能够有效降低私密信息的错误概率。根据分析结果,提出了一种利用信道衰落幅度差异隐藏私密信息的物理层安全编码方法,该方法针对合法信道最优化私密信息的位置选取,确保 Bob 对私密信息的可靠接收,而窃听信道由于衰落幅度图样不同于合法信道,私密信息位置对于 Eve 并非最优,所以 Eve 的错误概率高于 Bob;再通过私密信息置乱,在 Eve 端对私密信息的译码错误扩散,以此保证私密信息传输安全。衰落信道上的仿真结果表明,本方法在低 SNR 区域使 BER 迅速上升,在高 SNR 区域保证 Bob 可靠性的同时恶化 Eve 的接收性能,安全性能优于直接传输和仅私密信息置乱的方法。

### 参考文献


[1] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal,1975,54(8): 1355-1387.

[2] Shannon C. Communication theory of secrecy systems[J]. Bell Systems Technical Journal, 1949, 29: 656-715.

[3] Jiaxi Xiao, Xiaoli Ma, McLaughlin S W. Random complex field code design for securityover wiretap channels[C]// Proceedings of the IEEE International Conference on Information Science and Systems (CISS), 2011: 1-6.

[4] Byung-JaeKwak, Nah-Oak Song, Bumsoo Park,et al. Physical layer security with Yargcode[C]//Proceedings of the First International Conference on Emerging Network Intelligence, Taejon, 2009: 43-48.

[5] 王亚东, 黄开枝, 吉江. 一种多天线信道特征投影物理层安全编码算法[J]. 电子与信息学报, 2012, 34(7): 1653-1658.
Wang Yadong, Huang Kaizhi, Ji Jiang. A Physical Layer Secrecy Coding Algorithm Using Multi-antenna Channel Characteristics Projection[J]. Journal of Electronics & Information Technology, 2012, 34(7):1653-1658. (in Chinese)

[6] Klinc D, Ha J, Mclaughlin S W, et al. LDPC codes for physical layer security[C]//Proceedings of the Global Telecommunications Conference, Honolulu, America, 2009: 1-6.

[7] Klinc D, HaJeongseok, McLaughlin S W, et al. LDPC codes for the Gaussian wiretap channel[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3):532-540.

[8] Marco Baldi, Marco Bianchi, Franco Chiaraluce. Non-systematic codes for physical layer security[C]//Proceedings of the IEEE Information Theory Workshop, Dublin, Ireland, 2010: 1-5.

[9] Marco Baldi, Marco Bianchi, Franco Chiaraluce. Increasing physical layer security through scrambled codes and ARQ[C]//Proceedings of the IEEE International Conference on Communications, Kyoto, Japan, 2011:1-5.

[10] Marco Baldi. Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A Security Gap Analysis[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3):883-894.

[11] Kim H S. Measurement and model based characterization of indoor wireless channels[D]. USA: University of Massachusetts Lowell, Doctoral Dissertation,2003.

[12] 吴飞龙, 王文杰, 王慧明. 基于空域加扰的保密无线通信统一数学模型及其窃密方法[J]. 中国科学:信息科学, 2012, 42(4):483-492.
Wu Feilong, Wang Wenjie, Wang Huiming. A unified mathematical model for spatial scrambling based secure wireless communication and its wiretap method[J]. SCIENTIA SINICA Informationis, 2012, 42(4):483-492. (in Chinese)

[13] 李为, 陈彬, 魏急波,等. 基于接收机人工噪声的物理层安全技术及保密区域分析[J]. 信号处理, 2012, 28(9): 1314-1320.
Li Wei, Chen Bin, Wei Jibo,et al. Secure communication via sending artificial noise by the receiver: ergodic

secure region analysis[J]. Signal Processing, 2012, 28(9): 1314-1320. (in Chinese)

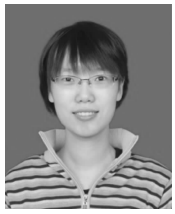
[14] Ishii S, Hoshikuki A, Kohno R. Space hopping scheme under short range Rician multipath fading environment [C]// Proceedings of the IEEE VTS-Fall Vehicular Technology Conference, Tokyo, 2000: 99-104.

[15] 殷勤业, 贾曙乔, 左莎琳,等. 分布式多天线跳空收发技术[J]. 西安交通大学学报, 2013, 47(1):1-8.
Yin Qinye, Jia Shuqiao, Zuo Shalin, et. al. A Distributed Multi-Antenna Space Hopping Transceiver Technique [J]. Journal of Xi'an Jiaotong University, 2013, 47(1):1-8. (in Chinese)

[16] Hou J, Siegel P, Milstein L. Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels[J]. IEEE Journal on selected Areas in Communications,2001, 19(5): 924-934.

[17] Ha J, Kim J, McLaughlin S. Rate-compatible Puncturing of Low Density Parity-check Codes[J]. IEEE Transactions on Information Theory, 2004, 50(11):2824-2836.

**作者简介**



**白慧卿**　女,1988 年生,河南洛阳人,博士研究生,主要研究方向为无线物理层安全技术。
E-mail:huiqingbai@163.com

**金　梁**　男,1969 年生,北京人,现为国家数字交换系统工程技术研究中心教授,博士生导师,主要研究领域为智能天线、无线与移动通信、超宽带通信、无线物理层安全技术等。E-mail:liangjin@263.com

**钟　州**　男,1980 年生,吉林省公主岭人,现为国家数字交换系统工程技术研究中心讲师,主要研究领域为无线与移动通信、超宽带通信、无线物理层安全技术等。
E-mail:zhongzhoundsc@gmail.com

**黄开枝**　女,1973 年生,安徽来安人,现为国家数字交换系统工程技术研究中心教授,博士生导师,主要研究领域为无线与移动通信、无线物理层安全技术、异构无线网络安全等。E-mail:huangkaizhi@tsinghua.org.cn