基于二维信息修正减小 LDPC 码安全间隙的译码算法

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

摘 要：该文通过分析安全编码的原理推导了安全间隙约束条件下高斯窃听信道保密速率的计算方法，并根据置信传播(Belief Propagation, BP)译码算法及其改进算法，针对基于中短码长 LDPC 码所设计的安全编码提出一种 2 维信息修正的分类归一化最小和译码算法。该算法先将输入校验节点信息绝对值分成最小值和次小值两类，然后在译码初始化时利用概率统计理论分别推导出相应的最佳归一化因子对分类后的信息进行修正。仿真结果表明，该算法在高信噪比区域的译码性能高于 BP 算法和归一化最小和算法，低信噪比区域误比特率迅速逼近 0.5，且能减小不同安全编码速率 LDPC 码的安全间隙，提高了保密信息安全传输的性能。

关键词：物理层安全编码；安全间隙；保密容量；窃听信道
中图分类号：TN918 **文献标识码：**A **文章编号：**1009-5896(2013)08-1946-06
DOI：10.3724/SP.J.1146.2012.01612

Decoding Algorithm for Reducing Security Gap of LDPC Codes Based on Two-dimensional Information Correction

Zhong Zhou Jin Liang Huang Kai-zhi Bai Hui-qing Yi Ming
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: This paper analyzes the mechanism of physical layer secrecy coding and calculates the secrecy rate for the Gaussian wiretap channel under the security gap constraint. Furthermore, a classified normalized decoding algorithm with two-dimensional information correction based on Belief Propagation (BP) algorithm and its improvements for the short and medium block length Low Density Parity Check (LDPC) based secrecy codes is presented. The algorithm first utilizes classification according to the absolute values of incoming messages in check nodes. Then it uses 2-dimensional normalization to correct the minimum and sub-minimum values. The 2-dimensional normalized factors can be calculated respectively by using probability and statistic theory in the initialization step. Simulation results show that the proposed algorithm achieves better performance than BP algorithm and normalized BP-based algorithm at the high SNR, but the bit error radio gets close to 0.5 rapidly at the low SNR. It can reduce security gap of LDPC-based secrecy codes with different secrecy rates efficiently.

Key words: Physical layer secrecy coding; Security gap; Security capacity; Wiretap channel

1 引言

安全编码(Secrecy Coding, SC)是在窃听信道模型[1]中，当在合法信道质量优于窃听信道质量的条件下，在物理层通过编码保证授权双方进行可靠通信的同时，使信息以逼近保密容量的速率进行安全传输的技术[2]。

目前由于LDPC码性能逼近Shannon限且具有较好的数学分析特性，近年来利用 LDPC 码构造物理层安全编码的研究成为热点。文献[3]使用安全间隙作为安全测度，提出了一种最小化安全间隙的打孔 LDPC 编码，该方法通过设计打孔图案将需要加密的信息比特打孔去除，接收时由于信道质量差异使得合法用户能够译码还原打孔位置隐藏的保密信息，而窃听者将因高误码率而无法正确恢复保密信息。Baldi 等人[4]将信息加扰与非系统 LDPC 码结合，通过设计满秩的信息置乱矩阵给出了一种非系统 LDPC 码的安全编码方法。随后又与混合自动反馈重传机制[5,6]结合，改进了窃听信道质量优于合法信道时的安全传输问题。文献[7]从调制星座映射的角度提出了一种以最大化相邻星座点的汉明距离为目的的“反格雷码”映射，通过扩大低信噪比区域的解调比特错误率，以达到缩小安全间隙的目的。文献[8]在瑞利快衰落窃听信道下，利用非规则 LDPC 码对保密通信中合法通信双方的密钥一致性进行研究，并基于密度进化理论提出了增强密钥一致性的最优度分布非规则 LDPC 码的设计方法。

上述方法从编码调制的角度基于无限码长的

2012-12-12 收到，2013-04-19 改回
国家自然科学基金(61171108)和国家 863 计划项目(2011AA010604)资助课题
*通信作者：钟州 zhongzhoundsc@gmail.com

LDPC 码设计安全编码，并采用置信传播(Belief Propagation, BP)译码算法，根据密度进化理论或高斯近似法对安全编码可达保密速率的极限性能进行了分析。然而实际通信过程中，一方面考虑通信系统编译码延迟对吞吐量的影响以及硬件实现复杂度等因素制约，发端需要采用中短码长的编码；另一方面，窃听者为了获取保密信息可以不计复杂度和计算资源实施窃听。这就需要我们针对有限码长的安全编码，不断为合法接收者设计高性能的译码算法以提高保密信息的还原能力。

2　物理层安全传输模型及安全编码基本原理分析

物理层安全传输模型主要涉及三方，如图 1 所示。发送端(记作 Alice)的保密信息 M 经过安全编码得到编码序列 X 后进行发送，该序列经过信道特征为 $\boldsymbol{H}_B$ 的信道到达合法用户(记作 Bob)，同时该发送序列受无线信道的广播特性经过信道特征为 $\boldsymbol{H}_E$ 的窃听信道被窃听者(记作 Eve)接收。Bob 和 Eve 分别通过对接收的序列进行译码而还原保密信息。当合法信道的质量占优时，存在保密容量如式(1)所示：

$$C_s = \max_{P_M}\left[I\left(M,\widehat{M}_B\right) - I\left(M,\widehat{M}_E\right)\right]^+ \tag{1}$$

从式(1)可以看出，Alice 与 Bob 之间的互信息 $I(M,\widehat{M}_B)$ 大于 Alice 与 Eve 之间的互信息 $I(M,\widehat{M}_E)$ 时，若以大于 $I(M,\widehat{M}_E)$ 的速率传输保密信息，则窃听者将无法完全获得保密信息的内容。反之，无论发送信号 M 服从任何分布，如果 $I(M,\widehat{M}_E)$ 大于 $I(M,\widehat{M}_B)$，此时 Bob 的安全信道容量为 0，即当 Bob 接收到的信号的信噪比低于 Eve 端接收信号的信噪比时，Bob 收到的任何信息在理论上都可被 Eve 接收还原，从而无法保证安全传输。实际通信中，考虑 Eve 可以采用多天线分集接收等方法获得较 Bob 更高的接收信号质量，因此上述合法信道质量占优的假设往往不能被满足。随机波束成形[9]以及人工噪声[10]等方法通过从总发射功率中分配部分功率，在发送的信号 M 中叠加与 $\boldsymbol{H}_B$ 正交的干扰信号，能够在不影响 Bob 接收信号质量的同时恶化 Eve 的接收信噪比。在此条件下，安全编码的引入可以有效地降低发端干扰功率，提高功率的利用率。

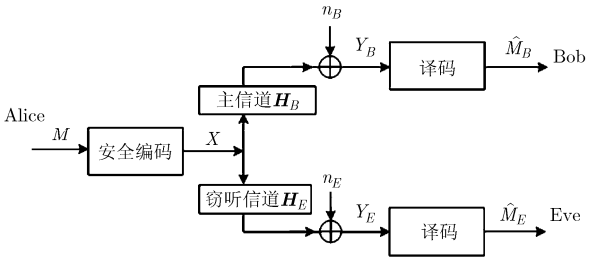

图 1 物理层安全传输模型

与传统信道编码(Channel Coding, CC)不同，安全编码的目标不仅是提高合法通信双方的可靠传输速率，使其逼近信道容量，还要最大化窃听者收到信息的不确定程度。这要求编译码在低信噪比区域具有极高的误码率而高信噪比区域误码率能迅速降低。文献[3]指出安全编码的性能可以用安全间隙进行度量。定义 $\mathrm{SNR}_{B,\min}$ 表示 Bob 能够以低于误码率 $P^B_{e,\max}$ 条件下进行可靠通信所需的最小信噪比门限，$\mathrm{SNR}_{E,\max}$ 表示 Eve 以误码率 $P^E_{e,\min}$ 几乎无法还原信息条件下(例如 $P^E_{e,\min}\approx 0.5$)保证信息安全传输所要求最大信噪比门限。若两个门限差值即安全间隙趋于零，那么当发端采用安全编码时，如果合法通信双方满足可靠通信条件，窃听信道质量只要比合法信道质量稍差一点就将无法还原发端的信息。为了建立该参数与文献[2]中所定义的保密速率的关系，给出如下定理。

定理　假设输入信号服从等概分布，定义二元熵函数 $H(e) = -e\log_2 e - (1-e)\log_2(1-e)$，用最大信道转移概率近似最大后验概率时，安全间隙约束条件下二进制高斯窃听信道的保密速率 $R_{SC} = 1 - h(P^B_{e,\max})$。

定理的证明略。

以文献[3]中保密信息打孔隐藏传输为例，现有基于 LDPC 码的安全编码均从编码设计角度出发，假设在无限码长且 Tanner 图中无短环条件下，研究采用无穷次迭代的 BP 译码算法时的安全性能。以上条件便于分析安全编码的安全性能理论限，但不适合实际应用。对于有限码长的 LDPC 码以及 Tanner 图中存在短环和陷阱集的情况，即使采用无限次迭代的 BP 译码也会因错误平台[11]的存在导致安全性能下降。因此，迫切需要我们对 BP 译码算法进行优化设计和改进，缩小安全间隙，降低对窃听者信道质量的约束，减小窃听信道质量占优条件下发端的干扰功率占总功率的比重，使信息的安全传输速率逼近保密容量。

3　基于 2 维信息修正的分类归一化最小和算法

3.1 迭代置信传播算法及简化算法分析

文献[12]证明了对码长无限的无短环 LDPC 码，BP 译码算法随迭代次数增加收敛于最大后验概率译码，是性能最优的译码算法，其计算步骤概括如下：

(1)计算变量节点的初始化信息：

$$L(P_i)^{(0)} = 2y_i/\sigma^2 \tag{2}$$

(2)计算校验节点的更新信息：

$$L(r_{ji}) = 2\tanh^{-1}\left(\prod_{i'\in R(j)\backslash i}\tanh\left(\frac{1}{2}L(q_{i'j})\right)\right) \tag{3}$$

(3)计算变量节点的更新信息：

$$L(q_{ij}) = L(P_i)^{(0)} + \sum_{j'\in C(i)\backslash j} L(r_{j'i}) \tag{4}$$

(4)译码判决：

$$\hat{m}_i = \begin{cases} 1, & L(Q_i) > 0 \\ 0, & L(Q_i) < 0 \end{cases} \tag{5}$$

其中 y_i 表示接收到的符号，该符号经编码调制后通过噪声方差为 σ^2 的信道。$R(j)\backslash i$ 表示与校验节点 j 相邻但不包含变量节点 i 的其余变量节点的集合，$C(i)\backslash j$ 表示与变量节点 i 相邻但不包含校验节点 j 的其余校验节点的集合。式(5)中参与判决的变量节点信息为 $L(Q_i) = L(P_i)^{(0)} + \sum_{j\in C(i)} L(r_{ji})$，若译码结果 $\hat{\boldsymbol{m}}$ 满足 $\boldsymbol{H}\cdot\hat{\boldsymbol{m}} = \boldsymbol{0}$，停止迭代并将 $\hat{\boldsymbol{m}}$ 作为译码结果输出，重复步骤(2)~步骤(4)进行迭代，超出最大迭代次数则表示译码失败。

定义 $L(q_{i'j}) = \phi_{i'j}\cdot\beta_{i'j}$，其中 $\phi_{i'j} = \mathrm{sign}(L(q_{i'j}))$，$(\beta_{i'j}) = |L(q_{i'j})|$，最小和算法对步骤(2)中式(3)的双曲正切运算做了如下简化[13]：

$$L(r_{ji}) = \left(\prod_{i'\in R(j)\backslash i}\phi_{ij}^{'}\right)\cdot\min_{i'\in R(j)\backslash i}(\beta_{i'j}) \tag{6}$$

将式(3)，式(6)的值分别记作 L_1, L_2，则 L_1, L_2 符号相同但 $|L_2| > |L_1|$。幅度的差异表明最小和算法相比 BP 算法在当输入到校验节点的信息相同的情况下过高估计了输出校验信息的可靠性。归一化最小和算法通过归一化处理修正节点取值概率的过估计值，将公式(6)修正为

$$L(r_{ji}) = \left(\prod_{i'\in R(j)\backslash i}\phi_{i'j}\right)\cdot\frac{1}{\alpha}\min_{i'\in R(j)\backslash i}(\beta_{i'j}),\quad \alpha>1 \tag{7}$$

通过分析最小和算法对 BP 算法的简化以及归一化最小和算法对于最小和算法的改进，可以发现当有限码长的 LDPC 码对应的 Tanner 图中存在短环，此时 BP 算法和最小和算法迭代译码过程中将存在正反馈，即错误信息通过短环进行扩散影响相邻节点的正确译码。此外，在采用最小和算法译码时，根据参与校验节点更新计算公式的约束条件 $R(j)\backslash i$，参与运算的信息既包含所有输入该校验节点信息绝对值的最小值记作 $Y_{\min 1}$，还包含次小值记作 $Y_{\min 2}$。归一化最小和算法显然在修正 $Y_{\min 1}$，$Y_{\min 2}$ 的信息幅度时采用了相同的归一化因子，而实际上每个校验节点输入的外信息是不同的，因此每个节点得到的修正因子也应不同。根据以上分析，考虑对 $Y_{\min 1}$ 和 $Y_{\min 2}$ 分类，分别计算对应的归一化因子进行 2 维修正，进而在高信噪比时得到更加精确的校验节点信息。

3.2 分类归一化最小和算法

假设 LDPC 码的校验矩阵行重为 d_c，那么对校验节点 j 的初始化输入信息 $\{L(P_{1j})^{(0)}, L(P_{2j})^{(0)}, \cdots, L(P_{d_cj})^{(0)}\}$ 取绝对值记为 $\{Y_1, Y_2, \cdots, Y_{d_c}\}$，它们是独立同分布的随机变量。下面对选择到最小值和次小值的情况进行分类，可建模为求顺序统计量的均值问题并按式(8)，式(9)计算 $Y_{\min 1}^{d_c}$，$Y_{\min 2}^{d_c}$ 的归一化因子。

$$\alpha_1 = \frac{E\left(Y_{\min 1}^{d_c}\right)}{E(|L_1|)} \tag{8}$$

$$\alpha_2 = \frac{E\left(Y_{\min 2}^{d_c}\right)}{E(|L_1|)} \tag{9}$$

首先根据式(10)计算 $|L_1|$ 的均值：

$$E(|L_1|) = E\left(\left|\ln\frac{1-\prod_{i=1}^{d_c-1}\dfrac{1-\exp(L(q_{ij}))}{1+\exp(L(q_{ij}))}}{1+\prod_{i=1}^{d_c-1}\dfrac{1-\exp(L(q_{ij}))}{1+\exp(L(q_{ij}))}}\right|\right) \tag{10}$$

将式(10)进行 Taylor 级数展开可得

$$E(|L_1|) = 2(m_1 + m_3/3 + m_5/5 + \cdots) \tag{11}$$

然后根据 $R(j)\backslash i$ 的约束条件计算 $|L_2|$ 的均值可表示为式(12)。

$$\begin{aligned} E(|L_2|) &= E\left(Y_{\min 1}^{d_c-1}\right) \\ &= \int_0^\infty\left[\int_y^\infty f_{Y_1}(y_1)\mathrm{d}y_1\right]^{d_c-1}\mathrm{d}y \\ &= \int_0^\mu\left[1-Q\left(\frac{\mu-y}{\sigma}\right)+Q\left(\frac{\mu+y}{\sigma}\right)\right]^{d_c-1}\mathrm{d}y \\ &\quad+\int_\mu^\infty\left[Q\left(\frac{y-\mu}{\sigma}\right)+Q\left(\frac{y+\mu}{\sigma}\right)\right]^{d_c-1}\mathrm{d}y \\ &\approx \int_0^\mu\left[1-Q\left(\frac{\mu-y}{\sigma}\right)+Q\left(\frac{\mu+y}{\sigma}\right)\right]^{d_c-1}\mathrm{d}y \end{aligned} \tag{12}$$

其中 $m_k = [E(\tanh(Y_1/2)^k)]^{d_c-1}$，$\mu = 4/N_0$，$\sigma^2 = 8/N_0$，$Q(x) = \left(1/\sqrt{2\pi}\right)\int_x^\infty e^{-x^2/2}\mathrm{d}x$。由式(12)计算 $Y_{\min 1}^{d_c}$ 的期望：

$$\begin{aligned} E\left(Y_{\min 1}^{d_c}\right) &= \int_0^\infty\left[\int_y^\infty f_{Y_1}(y_1)\mathrm{d}y_1\right]^{d_c}\mathrm{d}y \\ &= \int_0^\infty\left[1-F_Y(y)\right]^{d_c}\mathrm{d}y \\ &\approx \int_0^\mu\left[1-Q\left(\frac{\mu-y}{\sigma}\right)+Q\left(\frac{\mu+y}{\sigma}\right)\right]^{d_c}\mathrm{d}y \end{aligned} \tag{13}$$

$F_Y(y)$是$Y_1,Y_2,\cdots,Y_{d_c}$，的概率分布函数。其次令$a=y$, $b=y+\varepsilon,\varepsilon\to 0^+$，则由顺序统计量的性质可得

$$\begin{aligned}&\Pr\left(a<Y_{\min 2}^{d_c}\le b\right)=\frac{d_c!}{(d_c-2)!}\\&\quad\cdot F_Y(a)\left(1-F_Y(b)\right)^{d_c-2}\left(F_Y(b)-F_Y(a)\right)\end{aligned}\tag{14}$$

$$\begin{aligned}&f_{Y_{\min 2}^{d_c}}(y)\\&=\lim_{\varepsilon\to 0^+}\frac{F_Y(b)-F_Y(a)}{b-a}\\&=\lim_{\varepsilon\to 0^+}\left\{\left[\frac{d_c!}{\le\left(d_c-2\right)!}F_Y(y)\left(1-F_Y(y+\varepsilon)\right)^{d_c-2}\right.\right.\\&\quad\left.\left.\cdot\left(F_Y(y+\varepsilon)-F_Y(y)\right)\right]\Big/\varepsilon\right\}\\&=d_c(d_c-1)F_Y(y)(1-F_Y(y))^{d_c-2}f_Y(y)\end{aligned}\tag{15}$$

那么$Y_{\min 2}$的期望为

$$\begin{aligned}&\mathrm{E}(Y_{\min 2}^{d_c})\\&=\int_0^\infty y d_c\left(d_c-1\right)F_Y(y)\left(1-F_Y(y)\right)^{d_c-2}f_Y(y)\mathrm{d}y\\&=d_c\left(d_c-1\right)\int_0^\infty y\left[\left(1-F_Y(y)\right)^{d_c-2}\right.\\&\quad\left.-\left(1-F_Y(y)\right)^{d_c-1}\right]\mathrm{d}F_Y(y)\\&=d_c\int_0^\infty\left(1-F_Y(y)\right)^{d_c-1}\mathrm{d}y-\left(d_c-1\right)\\&\quad\cdot\int_0^\infty\left(1-F_Y(y)\right)^{d_c}\mathrm{d}y\end{aligned}\tag{16}$$

最后校验节点信息更新公式表示为

$$L\left(r_{ji}\right)=\begin{cases}\left(\prod\limits_{i'\in R(j)\backslash i}\phi_{i'j}\right)\cdot\dfrac{1}{\alpha_1}\min\limits_{i'\in R(j)\backslash i}\left(Y_{\min 1}^{d_c}\right),\\\quad\text{节点 }j\text{ 选中最小值}\\\left(\prod\limits_{i'\in R(j)\backslash i}\phi_{i'j}\right)\cdot\dfrac{1}{\alpha_2}\min\limits_{i'\in R(j)\backslash i}\left(Y_{\min 2}^{d_c}\right),\\\quad\text{节点 }j\text{ 选中次小值}\end{cases}\tag{17}$$

根据以上分析，基于 2 维信息修正的分类归一化最小和算法步骤如下：

(1)保持与 BP 算法相同的变量节点初始化信息计算方法；

(2)根据所有输入校验节点 j 的变量节点信息符号计算 $L(r_{ji})$ 的符号记作 $\prod_{i'\in R(j)\backslash i}\phi_{i'j}$，并求出该变量节点集合中绝对值的最小值$Y_{\min 1}^{d_c}$与次小值$Y_{\min 2}^{d_c}$，记录该值对应变量节点的位置；

(3)根据式(8)，式(9)的计算结果分别对 $Y_{\min 1}^{d_c}$，$Y_{\min 2}^{d_c}$进行 2 维修正；

(4)由步骤(2)和步骤(3)根据式(16)完成 $L(r_{ji})$ 的信息更新，然后保持 $L(q_{ij})$ 的计算不变完成一次迭代并进行译码判决。

考虑到归一化最小和算法的最佳归一化因子是根据 LDPC 码的度分布特性，在密度进化理论推导的译码门限所对应的信噪比处计算得到的。因此分类归一化最小和算法中的最佳修正因子 α_1，α_2 可同样根据归一化最小和算法在计算最佳归一化因子对应的信噪比处按式(8)，式(9)计算获得。

4　性能仿真与安全性能分析

本节利用 LDPC 码为母码构造安全编码，并根据该码参数计算分类归一化最小和算法的修正因子，以此分析改进译码算法的安全性能。不失一般性，首先按照 Mackay 随机构造校验矩阵方法[12,14]选择度分布多项式为 $d_c(x)=x^6,d_v(x)=x^3$，即行重 $d_c=6$，列重 $d_v=3$，生成码长 $n=2016$ 的规则 LDPC 母码，该码的编码效率为 0.5。然后，按照文献[3]中的打孔图样多项式 $\pi(x)=0.4x^3$，即采用对变量节点度为 3 的节点进行随机打孔 40%信息位的方法隐藏保密信息。记 α 为归一化最小和算法的归一化因子，α_1，α_2 分别为分类归一化最小和算法中 $Y_{\min 1}^{d_c}$，$Y_{\min 2}^{d_c}$ 对应的归一化因子。按照第 3 节提出的算法步骤，统计 0~5 dB 不同信噪比条件下接收到的符号样本值 y_i 计算出变量节点初始化信息，并利用式(8)，式(9)计算出 α_1，α_2 的值。其中计算 $E(|L_1|)$ 时，取式(11)的前 5 项作近似，在该条件下得到 α_1，α_2 随信噪比的变化曲线如图 2 所示。从图上可以看出归一化因子值随着信噪比的增加逐渐收敛为一个常数。同一信噪比处，分类归一化最小和算法所选用的两个归一化因子与归一化最小和算法所选的一个因子值是不相同的，这表明本文提出的算法对校验节点输入信息的最小值和次小值进行 2 维分类修正，相比归一化最小和算法的单一修正准则更加具有合理性。最后利用文献[15]中归一化最小和算法最佳归一化因子 α=1.25 对应的信噪比为 3.8 dB，相应地计算出分类归一化最小和算法的最佳修正因子 α_1=1.09，α_2=2.04。

定义 1　打孔效率 p 为由打孔图案删除的比特数 s 占编码后序列比特数 n 的比例，即 $p=s/n$；安全编码效率 R_s 为保密信息长度 d 占编码后有效传输编码长度 n' 的比例，即 $R_s=d/n'$，其中 $n'=(1-p)n$。

仿真首先设定 $p=0.4$，且所有被删除的比特都承载需要保密的信息，未被打孔删除的待编码信息则随机填充为 0 或 1，此时安全编码效率 $R_s=\dfrac{0.4n}{(1-0.4)n}=2/3$。对该安全编码分别采用 BP 算法，

归一化最小和算法和分类归一化最小和算法，设定最大迭代次数为 20 次进行安全性能比较。仿真通过独立收发 100000 帧由 BPSK 调制的数据，经过 AWGN 信道后对 Eve 接收还原保密信息的误比特率进行统计，结果如图 3 所示。为保证合法双方的可靠通信，设 $P^B_{e,\max} \le 10^{-6}$，可以看出当 Eve 的信道质量低于 Bob 时，所还原的保密信息误比特率迅速逼近至 0.5。根据不同安全等级的要求当 $P^E_{e,\min} = 0.4$ 时，分类归一化最小和算法得到的安全间隙为 1.6 dB，相比 BP 算法提高了 0.7 dB，而比归一化最小和算法提高了近 1 dB。这是因为中短码长 LDPC 码的校验矩阵对应的 Tanner 图上存在短环，使得迭代译码过程中外信息之间存在着一定的相关性，此时 BP 算法不再是最优的译码算法。3 种译码算法的误码率性能如图 4 所示，分类归一化最小和算法通过对输出校验信息的可靠性进行 2 维修正，减小正反馈对译码性能的影响，在中高信噪比区域改善了误码平层，使误比特率能快速下降至 $P^B_{e,\max}$；而在低信噪比区域，由于译码时打孔删除的变量节点不能为相邻校验节点提供任何信息，2 维修正又进一步降低了每个变量节点的置信概率，相比 BP 算法产生误码扩散形成较高的误码率，因此安全性优于归一化最小和算法并超越了 BP 算法。根据图 3 的仿真结果，若提高安全要求设 $P^E_{e,\min} \approx 0.5$，即达到使 Eve 几乎以猜的方式获取保密信息的效果时，3 种译码算法获得的安全间隙均趋于 6 dB。实际通信中 Alice 根据不同等级的安全要求，通过合理地设置干扰功率与发射功率能够以逼近保密容量的速率进行通信。

为了比较安全编码与信道编码在保密信息安全传输过程中的性能差异，我们选择与 IEEE WiMax 802.16e 标准[16]中的 LDPC 码直接传输保密信息的安全性能进行对比。仿真中保证保密信息传输效率的公平性，所选码字度分布多项式为 $d_v(x) = \frac{7}{24}x^2 + \frac{1}{2}x^3 + \frac{5}{24}x^6$，$d_c(x) = x^{10}$，码长 $n = 2304$，编码效率 $R_d = 2/3$，且待编码的信息比特都承载需要加密的信息，因此 $R_s = R_d = 2/3$。从图 3 中可以看出，Eve 在相同保密信息疑意度的约束条件下，信道编码(Channel Coding, CC)要比安全编码付出更多的干扰功率代价。

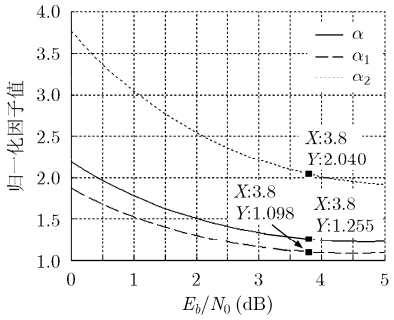

图 2 d_c=6, R=0.5 时归一化因子值

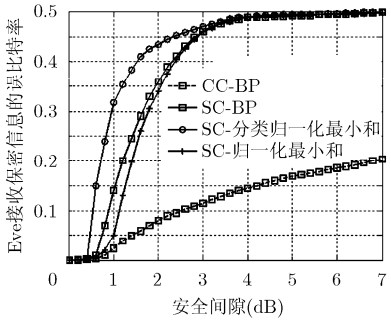

图 3 不同译码算法的安全性能

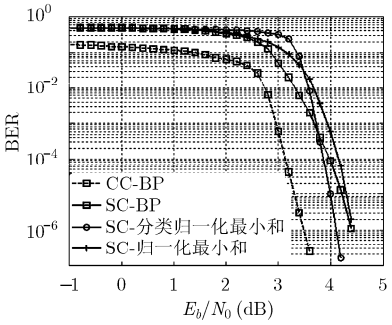

图 4 信道编码与不同译码算法下的安全编码的误码率性能

5 结论

本文针对物理层安全传输中采用基于打孔 LDPC 码构造安全编码的安全机理，以及中短码长的安全编码在译码时存在的问题，利用顺序统计量的分析方法，提出了基于校验节点 2 维信息修正的分类归一化最小和算法。该算法具有在中高信噪比区域误码率快速下降，低信噪比区域误码率快速逼近 0.5 的特点，因此在与其它基于 LDPC 码所设计的安全编码结合时均能提高安全传输速率。此外，即使本文提出的译码算法和打孔图案均被 Eve 窃取也能缩小安全间隙，这就迫使 Eve 也需要不断地寻找性能更优的译码算法以提高保密信息的截获能力。本文提出的算法还可以与传统基于应用层密钥的安全传输相结合，通过“一次一密”有效的增强无线通信中的安全，具有很好的应用价值。

参 考 文 献

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

[2] Csiszar I and Korner J. Broadcast channel with confidential messages[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 339–348.

[3] Klinc D, Jeongseok H, 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.

[4] Baldi M, Bianchi M, and Chiaraluce F. Non-systematic codes for physical layer security[C]. Proceedings of the IEEE Information Theory Workshop, Dublin, Ireland, 2010: 1–5.

[5] Baldi M, Bianchi M, and Chiaraluce F. Increasing physical

layer security through scrambled codes and ARQ[C]. Proceedings of the IEEE International Conference on Communications, Kyoto, Japan, 2011: 1–5.

[6] Baldi M. 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.

[7] Kwak Byung-jae, Song Nah-oak, Park Bumsoo, *et al.*. Physical layer security with Yarg code [C]. Proceedings of the First International Conference on Emerging Network Intelligence, Taejon, 2009: 43–48.

[8] Chan Wong-wong, Wong T F, and Shea J M. An LDPC-based key-agreement scheme over the fast-fading wiretap channel[C]. Proceedings of the 2011 IEEE International Conference on Military Communications, Florida, USA, 2011: 347–352.

[9] 吴飞龙, 王文杰, 王慧明, 等. 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 Fei-long, Wang Wen-jie, Wang Hui-ming, *et al.*. Aunified mathematical model for spatial scrambling based secure wireless communication and its wiretap method[J]. *SCIENTIA SINICA Information is*, 2012, 42(4): 483–492.

[10] Liao Wei-chen, Tsung Hui Chang, and Wing Kin Ma. Qos-based transmit beam forming in the presence of Eavesdroppers: an optimized artificial-noise-aided approach[J]. *IEEE Transactions on Signal Processing*, 2011, 59(3): 1202–1217.

[11] Chilappagari S K. Error floor of LDPC codes on the binary symmetric channel[C]. Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey, 2006: 1089–1094.

[12] MacKay D J C and Neal R M. Near Shannon limit performance of low density parity check codes[J]. *Electronics Letters*, 1996, 32(18): 1645–1646.

[13] Chen Jing-hu and Fossorier M P C. Near optimum universal belief propagation based decoding of low density parity check codes[J]. *IEEE Transactions on Communications*, 2002, 50(3): 406–414.

[14] MacKay D J C. David MacKay's Gallager code resources[OL]. www.interence.phy.cam. ac.uk/mackay/ gallager.html, 2008.

[15] Chen Jing-hu and Fossorier M P C. Density evolution for two improved BP-Based decoding algorithms of LDPC codes[J]. *IEEE Communication Letters*, 2002, 6(5): 208–210.

[16] IEEE 802.16e-2006. Air interface for fixed and mobile broadband wireless access systems[S]. 2006.

钟　州：　男，1982 年生，博士生，研究方向为信道编码、通信信号处理与信息论安全.

金　梁：　男，1969 年生，教授，研究方向为超宽带无线通信与智能天线.

黄开枝：　女，1973 年生，副教授，研究方向为宽带移动通信与异构无线网络安全.

白慧卿：　女，1988 年生，硕士生，研究方向为信道编码与通信信号处理.

易　鸣：　男，1986 年生，博士生，研究方向为通信信号处理与信息论安全.