基于网络编码和安全极化码的无线抗窃听传输技术

崔祥巍[1]，任清华[1]，李　蒙[1]，王　哲[2]
（1.空军工程大学信息与导航学院，西安，710077；
2.陆军装备部驻北京地区航空军事代表室，北京，100000）

摘要　由于无线通信的信道开放性和信号广播性，使其在服务合法用户的同时易受到非法用户的窃听。针对这一问题，结合网络编码技术和安全极化码技术，以随机线性网络编码对信源码块进行编码生成内码，通过计算极化码巴氏参数进行信道分集并选取安全比特信道，构造安全极化码作为外码，从而形成级联信道编码结构。仿真结果显示，当主信道信噪比为 10 dB 时，该方法与传统安全极化码都可以为合法接收方提供较好的通信服务；文中方法采用 8 bit 有限域时，只需窃听信道信噪比退化 2.5 dB，即可使得窃听信道的误码块率逼近 1，相较传统极化码方法所需的 4 dB 窃听信道信噪比退化，可更好地进行抗窃听传输。

关键词　抗窃听传输；安全极化码；网络编码
DOI　10.3969/j.issn.2097-1915.2022.06.013
中图分类号　TN957　　**文献标志码**　A　　**文章编号**　2097-1915(2022)06-0091-08

Anti-Eavesdropping Wireless Transmission Based on Network Coding and Secure Polar-Code Technology

CUI Xiangwei[1], REN Qinghua[1], LI Meng[1], WANG Zhe[2]
(1. Information and Navigation School, Air Force Engineering University, Xi'an 710077, China;
2. The Army Equipment Department Aviation Military Representative Office in Beijing, Beijing 100000, China)

Abstract　Wireless transmission being open in channel and broadcast in signals, there is a possibility to make legal users eavesdropped by illegal users in serving. In view of this question, the source code blocks are encoded with random linear network coding technology as inner codes in combination with network coding and polar-code technologies. Depending on Bhattacharyya-parameters, the channels are classified and the secure bit-channels are selected to structure secure a polar-code as outer codes to transmit internal codes, and a scheme of channel coding is adopted, carrying out concatenation of outer codes and inner codes. The simulation results show that when the SNR of the main channel is 10 dB, both of the proposed method and the traditional secure polar-code method can provide reliable communication service for the legitimate receiver. With this method adopting 8 bit finite field, only by degrading into 2.5 dB for the SNR of the eavesdropping channels can the block error rate of the eavesdropping channel approximate to 1, whereas the traditional polarization code method requires that the SNR of

收稿日期：2022-05-26
作者简介：崔祥巍(1994—)，男，吉林省吉林市人，硕士生，研究方向为无线物理层安全。E-mail:1617115329@qq.com

引用格式：*崔祥巍，任清华，李蒙，等.基于网络编码和安全极化码的无线抗窃听传输技术[J].空军工程大学学报，2022，23(6)：91-98. CUI Xiangwei，REN Qinghua，LI Meng，et al. Anti-Eavesdropping Wireless Transmission Based on Network Coding and Secure Polar-Code Technology[J]. Journal of Air Force Engineering University，2022，23(6)：91-98.*

the eavesdropping channel degrades by 4 dB. Compared with the traditional method, the proposed method can further resist eavesdropping transmission.

Key words anti-Eavesdropping transmission; secure polar-code; network coding

自 2008 年 Arikan 提出极化码这一可达香农极限的信道编码技术以来，极化码技术已广泛应用于光通信[1]、水声通信[2]等领域无线通信，并被确定为 5G 技术增强型移动宽带场景下的控制信道编码。由于其编码过程即是信道极化过程，在降低编、译码复杂度的同时也提升了与信道特征的匹配[3]。基于极化码的这些特点，学术界运用极化码技术开展的安全编码研究已取得了一系列成果。文献[4]通过比特信道估算，进行信道分集，选取安全信道集合构造安全极化码用于无线通信。文献[5]通过理论分析与仿真研究了兼顾安全性与有效性的消息比特数取值范围。文献[6]提出了基于极化码的密钥协商方法，通过仿真测试证明相对基于低密度奇偶校验码(low density parity check code，LDPC)的密钥协商方法，基于极化码的密钥协商方法的密钥协商效率更高。文献[7]在随机线性码加密方案的基础上，利用极化码的信道极化特性，提出了一种考虑语义安全性、抗自适应选择密文攻击的改进公钥加密方案。文献[8]利用极化码技术为非正交多址接入(non-orthogonal multiple access，NOMA)系统提供安全传输方案。

此前一些研究已经将网络编码技术与极化码技术进行了结合，利用其在可扩展性、吞吐量、节点能耗等方面的优势，优化移动自组网性能。文献[9]提出了一种基于极化码的网络编码协作通信方案，以极化码作为承载网络编码的码字，应用于多信源多中继的网络拓扑中，进一步提升通信系统的转发效率，降低通信节点能量和资源消耗，通过扩展可以更好地应用于移动自组网。在文献[10]中，专门针对双向中继通信提出了物理层网络编码和极化码的联合设计方案，并通过仿真得出相对 LDPC 码具有低译码复杂度和低计算量的优势。

在无线通信中，网络编码的内生安全性能高度依赖多径分集增益和中继节点对多源信号的叠加[11]。当窃听方能够对发送方、中继节点与接收方之间的所有信道进行窃听时，网络编码系统安全性能较弱，通常需要与公钥加密等技术相结合以提升抗窃听能力，这对无线通信设备提出了苛刻的计算能力需求和能耗需求。针对以上问题，本文将安全极化码与网络编码相结合，从抗窃听通信的角度展开研究，构建场景模型进行仿真实验，测试基于网络编码和安全极化码的无线抗窃听传输技术。

1 场景模型

如图 1 所示，本场景模型衍生自高斯退化窃听模型，以 Alice 作为发送方生成信源信号 $\boldsymbol{M}$，经过网络编码译码器进行编码作为外码，经安全极化码进行信道编码生成内码 $X^{1:N}$ 后发出。为了模拟窃听方能够以信噪比略低于合法信道的代价窃听所有信源-中继节点、中继节点-信宿、信源-信宿的信道，进而使得网络编码系统丧失分集增益这一极端情况，本模型简化了中继节点环节，模拟信号在加性高斯噪声(additive white Gaussian noise，AWGN)信道中传输。Bob 作为接收方将收到的信号 $Y^{1:N}$ 经过极化码译码和网络编码译码后还原后得到信源信号。Eve 作为窃听方将其接收到的信号 $Z^{1:N}$ 经相同的译码操作得到信源信号 $\hat{\boldsymbol{M}}'$。

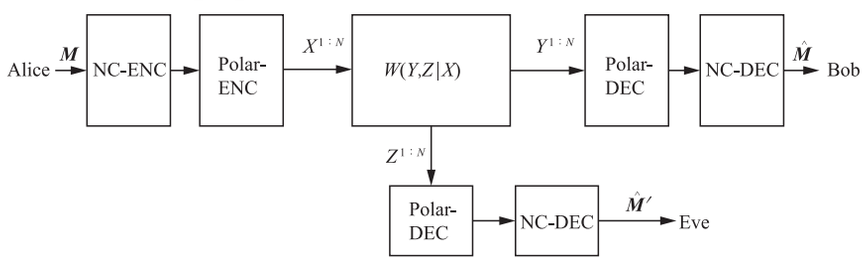

图 1 场景模型示意图

2 基本原理

2.1 网络编码

文献[11]指出随机线性网络编码可以很好地适应现实网络拓扑结构的灵活性和可实现性需求。其简要编、译码原理如下。

1)编码过程：发送方 Alice 将信源数据 $\boldsymbol{M}$ 分为 k 个数据块 $\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_k$，从有限域 GF($p$)中随机选取 k^2 个元素作为编码系数并构成编码矩阵 $\boldsymbol{L}$，其中

p 表示有限域的元素数量，此处需保证由编码矩阵 $\boldsymbol{L}$ 是一个可逆矩阵。编码过程是利用有限域矩阵乘法运算 $\boldsymbol{X}=\boldsymbol{L}\cdot\boldsymbol{M}$ 获取网络编码后的数据矩阵 $\boldsymbol{X}$。

$$\begin{pmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\\ \vdots\\ \boldsymbol{x}_k\end{pmatrix}=\begin{pmatrix}\boldsymbol{l}_{11} & \boldsymbol{l}_{12} & \cdots & \boldsymbol{l}_{1k}\\ \boldsymbol{l}_{21} & \boldsymbol{l}_{22} & \cdots & \boldsymbol{l}_{2k}\\ \vdots & \vdots & & \vdots\\ \boldsymbol{l}_{k1} & \boldsymbol{l}_{k2} & \cdots & \boldsymbol{l}_{kk}\end{pmatrix}\begin{pmatrix}\boldsymbol{m}_1\\ \boldsymbol{m}_2\\ \vdots\\ \boldsymbol{m}_k\end{pmatrix} \tag{1}$$

将 $\boldsymbol{l}_{11},\boldsymbol{l}_{12},\cdots,\boldsymbol{l}_{1k}$ 与 x_1 串接为 Alice 发出的第 1 个数据块，重复这样的串接操作将后面 $k-1$ 个数据块发出。

2）译码过程：接收方 Bob 从收到的 k 个数据块中获取数据矩阵 $\hat{\boldsymbol{X}}$ 和编码矩阵 $\hat{\boldsymbol{L}}$。通过有限域计算获取编码矩阵 $\hat{\boldsymbol{L}}$ 的逆矩阵 $\hat{\boldsymbol{L}}^{-1}$。译码过程是利用矩阵乘法运算 $\hat{\boldsymbol{M}}=\hat{\boldsymbol{L}}^{-1}\cdot\hat{\boldsymbol{X}}$ 获取信源信息 $\hat{\boldsymbol{M}}$。

$$\begin{pmatrix}\hat{\boldsymbol{m}}_1\\ \hat{\boldsymbol{m}}_2\\ \vdots\\ \hat{\boldsymbol{m}}_k\end{pmatrix}=\hat{\boldsymbol{L}}^{-1}\begin{pmatrix}\hat{\boldsymbol{x}}_1\\ \hat{\boldsymbol{x}}_2\\ \vdots\\ \hat{\boldsymbol{x}}_k\end{pmatrix} \tag{2}$$

欲实现式(2)中的译码过程必须保证接收方所收到的编码矩阵 $\hat{\boldsymbol{L}}$ 的秩为 k，才能实现矩阵可逆。当矩阵不可逆时，整个数据矩阵 $\hat{\boldsymbol{X}}$ 也将无法译码，从而无法获取信源信息 $\hat{\boldsymbol{M}}$。

接收方欲获取正确的信源信息 $\boldsymbol{M}$，则需要接收正确的编码数据矩阵 $\boldsymbol{X}$ 和正确的编码矩阵 $\boldsymbol{L}$。

2.2　高斯信道下极化码的构造方法

Arikan 在提出极化码时，给出了二元输入离散无记忆(binary discrete memoryless channel，BDMC)信道 W_{B} 中的构造方法。对于阶数为 n 的极化码，其码块长 N 为 2^n，可分裂为 2^n 个子信道。再通过分组迭代进行信道联合。

如图 2 所示，一个长度为 2 的极化码是极化码的基本组成模块。

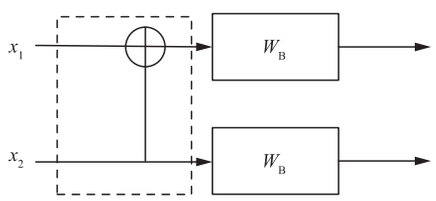

图 2　码块长为 2 的极化码

这一基本模块中，2 条子信道的转移概率可通过式(3)～(4)进行计算。在公式中可以观察到此时 2 条子信道 $W_2^{(1)}$ 和 $W_2^{(2)}$ 的转移概率分别出现了上升、下降的变化。

$$W_2^{(1)}(y_1^2\mid x_1)=$$

$$\frac{1}{2}\sum_{x_2}W_{\mathrm{B}}(y_1\mid x_1\oplus x_2)W_{\mathrm{B}}(y_2\mid x_2) \tag{3}$$

$$W_2^{(2)}(y_1^2,x_1\mid x_2)=$$

$$\frac{1}{2}W_{\mathrm{B}}(y_1\mid x_1\oplus x_2)W_{\mathrm{B}}(y_2\mid x_2) \tag{4}$$

如图 3 所示，在构造 2 阶极化码时，运用 2^{n-1} 个参照基础组成模块进行相似信道联合。同理在构造 n 阶极化码，皆从 2 个 2^{n-1} 阶极化码联合构造而来。在单一子信道中延续式(3)～(4)中的变化规律。当 n 的数值趋近于无穷时，信道转移概率将呈现出两极分化的现象。

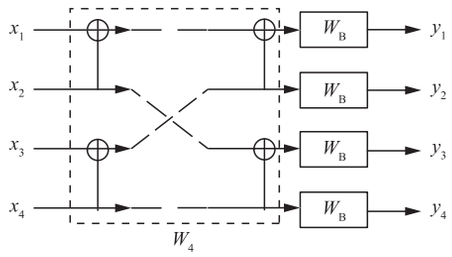

图 3　码块长为 4 的极化码

在接收方可以通过逆运算，迭代进行信道分裂，从而进行极化码译码获取信息。

Arikan 定义巴氏(Bhattacharyya)参数 $Z(W_{\mathrm{B}})$ 作为在信道 W_{B} 中传输一次 0 或 1 是采用最大似然准则判决的误比特概率上界。其计算方法见式(5)：

$$Z(W_{\mathrm{B}})=\sum_{y\in Y}\sqrt{W_{\mathrm{B}}(y\mid 0)W_{\mathrm{B}}(y\mid 1)} \tag{5}$$

式中：$W_{\mathrm{B}}(y|x)$ 表示信道 W_{B} 的信道转移概率；y 表示输出比特。

基于已知的子信道逻辑关系可以迭代计算各子信道的巴氏参数，通过计算选取其中 $Z(W_{\mathrm{B}})$ 较小的比特信道组成集合传输信息比特，其余的比特信道传输冻结比特。

但在 AWGN 信道 W 中，信道转移概率 $W(y|x)$ 受噪声影响，须进行估算方可构建极化码。本文采用高斯近似法估算各比特信道在 AWGN 信道中的巴氏参数。当信道 W 的噪声方差为 σ^2 时，第 i 个比特信道的信道转移概率对数似然比 $LLR_n^{(i)}$，计算方法为：

$$LLR_n^{(i)}=\log\frac{W(y\mid 0)}{W(y\mid 1)} \tag{6}$$

$LLR_n^{(i)}$ 的概率密度服从高斯分布：

$$N\left(\frac{2}{\sigma^2},\frac{4}{\sigma^2}\right) \tag{7}$$

第 i 个比特信道的对数似然比对应的分布均值 $m_n^{(i)}$ 可根据密度进化的递归定义计算：

$$m_n^{(2)}=2m_{n/2}^{(j)} \tag{8}$$

$$m_n^{(2j-1)}=f^{-1}(1-(1-f(m_{n/2}^{(j)}))^2) \tag{9}$$

迭代初值为：

$$m_1^{(1)}=\frac{2}{\sigma^2} \tag{10}$$

文献[12]给出了函数 $f(x)$ 的近似表示：

$$f(x)=\begin{cases}\mathrm{e}^{\alpha x^{\gamma}+\beta}, & x<10\\ \frac{1}{2}\left(\sqrt{\frac{\pi}{x}}\,\mathrm{e}^{-\frac{x}{4}}\left(1-\frac{3}{x}\right)+\sqrt{\frac{\pi}{x}}\,\mathrm{e}^{-\frac{x}{4}}\left(1+\frac{1}{7x}\right)\right), & x\geqslant 10\end{cases} \tag{11}$$

式中：$\alpha=-0.452\ 7$；$\beta=0.021\ 8$；$\gamma=0.86$。

令 $(\sigma_n^{(i)})^2$ 表示第 i 个比特信道 $W_n^{(i)}$ 的噪声方差，可通过式(12)计算：

$$(\sigma_n^{(i)})^2=\frac{2}{m_n^{(i)}} \tag{12}$$

在作为连续信道的 AWGN 信道中计算巴氏参数 $Z(W)$ 方法为：

$$Z(W)=\int_{-\infty}^{\infty}\sqrt{W(y\mid 0)W(y\mid 1)}\,\mathrm{d}y=$$

$$\int_{-\infty}^{\infty}\sqrt{\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{-\frac{(y-1)^2}{2\sigma^2}}\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{-\frac{(y+1)^2}{2\sigma^2}}}\,\mathrm{d}y=\mathrm{e}^{-\frac{1}{2\sigma^2}} \tag{13}$$

在比特信道噪声方差 $(\sigma_n^{(i)})^2$ 已知时，可利用式(13)得到第 i 个比特信道 $W_n^{(i)}$ 的巴氏参数：

$$Z(W_n^{(i)})=\mathrm{e}^{-\frac{1}{2(\sigma_n^{(i)})^2}} \tag{14}$$

在计算出所有比特信道的巴氏参数后，与 BDMC 信道中的方法类似，选取其中巴氏参数较小的传输信息比特，其余的比特信道传输冻结比特。

2.3 安全极化码的构造方法

在高斯退化窃听信道中，窃听信道的噪声方差 σ_{E}^2 大于合法信道噪声方差 σ_{B}^2，由式(14)计算得到 2 个信道中各比特信道的巴氏参数差值，可知极化结果存在差异。利用这一差异，可将比特信道分为 3 类：①对于合法接收方和窃听方都有较高可靠性的比特信道集合 R，通常用于传输公开信息或加密后的信息；②信道极化结果对合法接收方较为可靠但对窃听方性能较差的比特信道集合 B，通常用于传输密钥或私密信息；③对合法接收方和窃听方皆质量较差的比特信道集合 F，通常用于传输冻结比特。参考文献[13]中已经给出了一种安全门限的计算方法，参照式(15)～(17)将合法接收方和窃听方 2 种 AWGN 噪声方差条件下的各比特信道巴氏参数与门限值 $2^{-n^{\omega}}/n$ 进行对比，其中 ω 为常数，取值范围为[0，0.5)。

$$R\triangleq\left\{i\in[n]:Z_{\mathrm{B}}(W_i)<\frac{2^{-n^{\omega}}}{n},Z_{\mathrm{E}}(W_i)<\frac{2^{-n^{\omega}}}{n}\right\} \tag{15}$$

$$B\triangleq\left\{i\in[n]:Z_{\mathrm{B}}(W_i)<\frac{2^{-n^{\omega}}}{n},Z_{\mathrm{E}}(W_i)\geqslant\frac{2^{-n^{\omega}}}{n}\right\} \tag{16}$$

$$F\triangleq\left\{i\in[n]:Z_{\mathrm{B}}(W_i)\geqslant\frac{2^{-n^{\omega}}}{n},Z_{\mathrm{E}}(W_i)\geqslant\frac{2^{-n^{\omega}}}{n}\right\} \tag{17}$$

通过巴氏参数的定义可知，当常数 ω 在取值范围内越大时，门限内 $Z_{\mathrm{B}}(W_i)$ 的取值越小，合法接收方的通信可靠性越高；当常数 ω 在取值范围内越小时，门限内 $Z_{\mathrm{B}}(W_i)$ 的取值越大，合法接收方的通信可靠性越低，同时窃听方的误比特概率越大，传输安全性越高。

通过以上叙述可以了解到，这种方法需要合法信道与窃听信道之间的信噪比差额尽量大，方可为发送方提供足够多的安全子信道来构造集合 B。在文献[5]中，还证明了当极化码的阶数 n 趋近于无穷时，集合 B 中的安全子信道也将趋于无穷，采用这一方法可以实现弱安全。但这些条件在实际通信过程中往往难以实现，严重制约了系统的抗窃听性能。

3 基于网络编码和安全极化码技术的抗窃听传输

文献[14]利用椭圆加密算法将网络编码的编码系数加密为 $\boldsymbol{K}$，使得窃听方难以从密文窃听值 $\hat{\boldsymbol{K}}'$ 得到编码矩阵 $\hat{\boldsymbol{L}}'$，且与传输编码矩阵 $\boldsymbol{L}$ 对比出现差错的概率大，进而难以获得正确的逆矩阵 $\boldsymbol{L}^{-1}$，进而无法利用式(2)获取 $\boldsymbol{M}$。相较于传统对全部信源信息进行加密的方法，这种方法运算量大幅降低，但是使用密码学加密算法，计算复杂度依旧较大，达到 $O(k^2p)$。

借鉴于这种思路，本方法从安全信道编码的角度，利用安全极化码技术选取符合可靠和安全标准的极化码比特信道组成集合 B，用于传输编码矩阵 $\boldsymbol{L}$。如此，可以将安全极化码和网络编码技术在信息论层面的安全性能相结合，进一步提升抗窃听能力。

3.1 外码生成过程

1)构建有限域 GF(p)，从其中选取 k^2 个元素构成系数矩阵 $\boldsymbol{L}$，并检验这一矩阵在有限域中是否可逆。如果不可逆，则重新生成系数矩阵 $\boldsymbol{L}$。

2)将信源数据 $\boldsymbol{M}$ 分解为 k 个数据块，在此处需注意各数据块的长度应当为 $\log_2 p$ 的正整数倍以便后续计算，这里假设这一倍数为 a。

3)将 k 个数据块中，每 $\log_2 p$ 个比特双射映射为有限域 GF(p)中的元素，构成一个 k 行的信源矩阵 $\boldsymbol{M}_{\mathrm{GF}}$。

4)系数矩阵 $\boldsymbol{L}$ 与信源矩阵 $\boldsymbol{M}_{\mathrm{GF}}$ 在有限域 GF(p)中进行矩阵乘法获得编码后的信源信息矩阵 $\boldsymbol{X}$。

5)将编码系数矩阵 $\boldsymbol{L}$ 的行向量与编码后的信源

信息矩阵 $\boldsymbol{X}$ 的行向量串接，形成 k 个外码信息码块。

3.2 内码生成及传输过程

1）首先运用 2.2 节中所提到的式(6)～(14)迭代估算 2^n 个子信道的巴氏参数 $Z(W_n^{(i)})$。

2）将各子信道的巴氏参数 $Z(W_n^{(i)})$ 逐一与门限值 $2^{-n^{\omega}}/n$ 进行对比，按照式(17)将合法信道信噪比条件下巴氏参数超过门限值的子信道划入 F。

3）对剩余的子信道按照巴氏参数进行排序，选取其中巴氏参数最大的 $k\log_2 p$ 个子信道构成拟集合 B'。

4）从剩余的子信道中，选取巴氏参数最小的 $a\log_2 p$ 个子信道构成集合 R'。

5）将外码信息码块中的编码矩阵信息编入集合 B' 中的子信道，将外码信息码块中编码后的信源信息编入集合 R' 中的子信道，在其余的子信道编入校验信息和冻结比特，从而构成 k 个经过安全极化码编码的内码码块，随后发出这些码块。

3.3 接收方译码过程

1）按照 2.2 节中所提到的迭代算法还原出个子信道中所承载的信息。

2）通过校验算法检验接收到的信息是否存在错误：如无误，进入下一步骤；如有误，合法接收方可申请重传。

3）构建相同的有限域 GF(p)，在接收到 k 个码块后，检验接收到的编码矩阵 $\hat{\boldsymbol{L}}$ 在有限域中是否可逆，如可逆则利用 $\hat{\boldsymbol{L}}^{-1}$ 与接收到的编码后的信源信息矩阵 $\hat{\boldsymbol{X}}$ 进行有限域内的矩阵乘法，获取信源矩阵 $\hat{\boldsymbol{M}}_{\mathrm{GF}}$，利用双射转换关系获取信源数据 $\boldsymbol{M}$。

4）如矩阵 $\hat{\boldsymbol{L}}$ 在有限域内不可逆，则合法接收方可申请重传，窃听方欲强行破解则需在有限域 GF(p)随机生成可逆矩阵 $\boldsymbol{L}_{\mathrm{E}}$ 后参照步骤 3）中的方法进行译码。

3.4 性能分析

为了在实际通信中，令窃听方以尽可能小的信道退化幅度，产生尽可能高的窃听方误码率(bit error rate，BER)和误码块率(block error rate，BLER)，选取巴氏参数 $Z(W_n^{(i)})$ 较高的子信道构成集合 B'，因为这些信道可在尽可能小的信道退化幅度下符合式(16)中集合 B 的条件。对于窃听方接收集合 B 的信息存在更高的误比特率，当窃听方接收到的编码矩阵 $\hat{\boldsymbol{L}}'$ 出现错误时，无论能否求逆，窃听方都将大概率以错误的编码矩阵 $\hat{\boldsymbol{L}}'$ 和 $\boldsymbol{L}_{\mathrm{E}}$ 进行网络编码译码，这会造成误码扩散。当错误码块中的错误比特全部集中于编码矩阵 $\hat{\boldsymbol{L}}'$ 时，伴随网络编码译码涉及到矩阵逆的扰动，将大幅度影响误码率。当接收方误码全部集中于信源信息部分内容时，由矩阵乘法易知，接收方所得到的信源矩阵 $\hat{\boldsymbol{M}}_{\mathrm{GF}}$ 对应列的元素将出现错误，误码扩散到所有码块，也将带来一定的误码率扩散。假设窃听方接收每一码块的错误概率为 $bler_{\mathrm{El}}$，则利用 k 个码块还原信源信息的误码块率最高可达到 $1-(1-bler_{\mathrm{El}})^k$。

使用这一方法能够绕过传统密码学方法对于复杂计算能力和安全密钥分发的要求，只需在传统依托极化码的网络编码系统基础上，进行安全极化码信道选取，计算复杂度为 $O(n)$。在数据分块的首部需要付出 $k\log_2 p$ bit 的首部开销，在空间复杂度要 k 倍于传统安全极化码。

4 仿真测试与结果分析

4.1 仿真参数设置

仿真实验中，模拟极化码承载信息码块($\boldsymbol{L};\boldsymbol{N}$)，长为 512 bit，采用 crc-16 校验，从有限域 GF(2^4)、GF(2^8)、GF(2^{16})中选取网络编码系数对信源信息进行网络编码。极化码的阶数设置为 10，极化码块长为 1 024 bit，可分裂为同样数量的子信道。为了在构造安全极化码的同时保障合法接收方的通信性能，将安全极化码门限常数 ω 设置为 0.2。可通过 $2^{-n^{\omega}}/n$ 计算，得出巴氏参数门限值约为 $6.103\,5\times10^{-5}$。接收方和窃听方均采用 SCL 方法进行极化码译码，其中译码缓存表位数为 16 位。

由于本文所采用的场景模型为高斯退化信道，所以窃听方信噪比条件小于等于合法接收方的信噪比。为了在测试抗窃听能力的同时观察合法接收方通信可靠性本文在高信噪比场景中，合法信道的信噪比为 10 dB，窃听信道的信噪比取 6～10 dB；在低信噪比场景中，合法信道的信噪比为 5 dB，窃听方的信噪比取 3～5 dB。模型模拟发送 1 000 个码块。

4.2 仿真结果及分析

仿真测试主要包括：①运用高斯估计法分别对高信噪比和低信噪比场景下极化码子信道的巴氏参数进行估计；②以门限值对于 2 种场景下的极化码子信道进行分集，选取安全信道；③模拟传输信息，以窃听方误码率、误码块率对比测试安全极化码和本方法的安全性能。

如图 4 所示，在子信道分集之前，首先使用式

(14)对极化码的所有子信道巴氏参数进行估算。可以看到同一子信道在信噪比由高至低的条件下,其巴氏参数逐渐增大,其误比特概率上界逐渐提高。存在部分子信道在信噪比 10 dB 时,巴氏参数低于门限值,伴随着窃听信道退化程度逐渐加深巴氏参数超门限值,从而产生了符合式(16)中条件的安全子信道。由于实验场景的信噪比较高,多数子信道的巴氏参数已经低于 10^{-10}。

图 5 截取 7～10 dB 信噪比条件下超出门限的子信道。如图 5 所示,在 10 dB 的合法信道中只有 6 个子信道的巴氏参数高于门限值,这些信道对于合法信道和窃听信道的可靠性都不理想,划分到集合 F。伴随着窃听信道的信噪比逐渐降低,超出门限值的子信道数量逐渐增加。在这里去除已经被划入集合 F 的 6 个子信道,其他超出门限的子信道符合式(16)中集合 B 的条件。

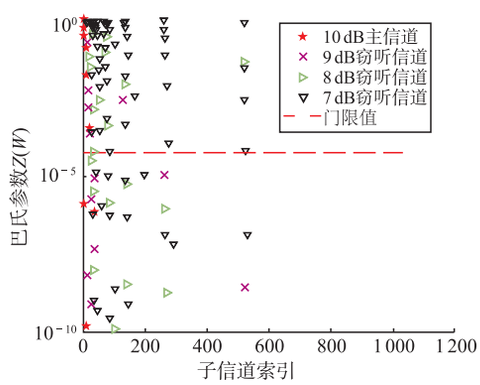

图 4 不同信噪比下子信道巴氏参数

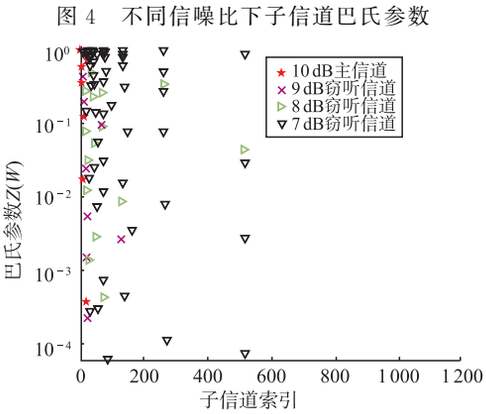

图 5 不同信噪比下超出门限的子信道

表 1 合法接收方 2 种场景下不同有限域误码率对比

有限域	高信噪比场景	低信噪比场景
GF(2^{16})	0.000 368 743	0.003 748 20
GF(2^{8})	0.000 000 000	0.002 004 80
GF(2^{4})	0.000 000 000	0.000 833 33

如表 1 所示,本方法采用不同的有限域在合法接收方的 10 dB 信噪比条件下都可以取得较好误码率性能。但在仿真测试中,使用 GF(2^{16})的合法接收方误码率高于采用 GF(2^{8})、GF(2^{4})的合法接收方误码率。

图 6 中在不同大小的有限域中使用本方法测试,伴随着有限域的逐渐增大,相同信噪比条件的窃听方解码后获得的误码概率也逐渐增大。

分析这种情况主要是由于此时编码矩阵 $\boldsymbol{L}$ 较大,在内码码块生成过程中使用了较 GF(2^{4})和 GF(2^{8})使用了更多巴氏参数 $Z(W_n^{(i)})$ 较高的子信道,增大了出现误码的概率,而且错误将在 16 个同组码块中扩散,也进一步增大了误码率。当窃听方信噪比为 7.5 dB 时,采用本方法可使窃听方误码率约为 0.5,已经接近于随机概率。而传统的安全极化码在所选取的信噪比范围中,误码率最高约为 0.1。

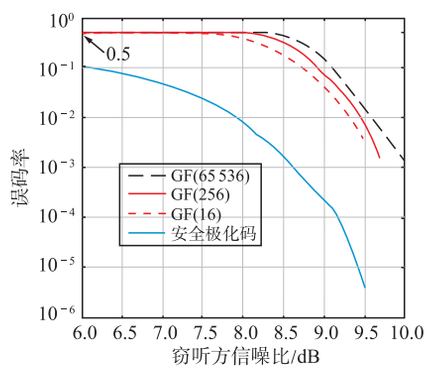

图 6 高信噪比场景下窃听方误码率对比图

如表 2 所示,本方法在合法接收方都可以取得较好误码块率性能,可以在通信系统广泛采用的 10 dB 信噪比指标下为合法接收方提供性能较佳的服务。当采用 GF(2^{16})时,合法接收方的误码块率高于采用 GF(2^{8})、GF(2^{4})时的误码块率。

表 2 合法接收方两种场景下不同有限域误码块率对比

有限域	高信噪比场景	低信噪比场景
GF(2^{16})	0.000 740 741	0.007 500 00
GF(2^{8})	0.000 000 000	0.004 000 00
GF(2^{4})	0.000 000 000	0.000 420 53

图 7 中在当窃听方信道的信噪比在 9.5～10 dB 之间且有限域为 GF(2^{4})、GF(2^{8})时,由于此时窃听信道退化幅度较低,达到集合 B 标准的安全子信道数量较少,网络编码技术将误码扩散至相邻码块的效率较低。即使按照理论最大值 $1-(1-bler_{\mathrm{El}})^{k}$ 计算,在高信噪比场景下窃听信道退化幅度有限时接收单一码块的错误概率 $bler_{\mathrm{El}}$ 趋近于 0,窃听方误码块率 $bler_{\mathrm{E}}$ 趋近于 0。此时本方法与安全极化码之间的误码块率性能差别不大,抗窃听性能较差。采用本方法可以在窃听方信噪比为

9 dB 时实现 0.1 的误码块率。这一数值通常被作为 5G 和 LTE 数据网络的误码块率上界。而此条件下采用传统安全极化码时，窃听方误码块率逼近 0.02，抗窃听性能较差。

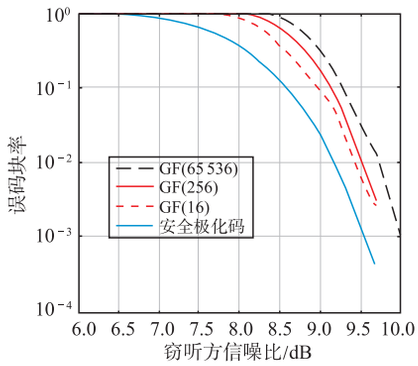

图 7　高信噪比场景下误码块率对比图

在低信噪比场景下，同样利用高斯估算法估测所有子信道的巴氏参数。从图 8 可以看到，与高信噪比场景相对比，在低信噪比场景下，各子信道的巴氏参数 $Z(W_n^{(i)})$ 更高，有更多的子信道巴氏参数超出门限值。如果继续按照此前在高信噪比场景下选取的子信道进行传输，极化码的误码率会大幅度上升，结合网络编码码性质造成的误码扩散会大幅度提高误码率和误码块率，严重降低通信可靠性。此时，需要通过与门限值对比再次进行信道分集，重新选取适应低信噪比场景的安全子信道。

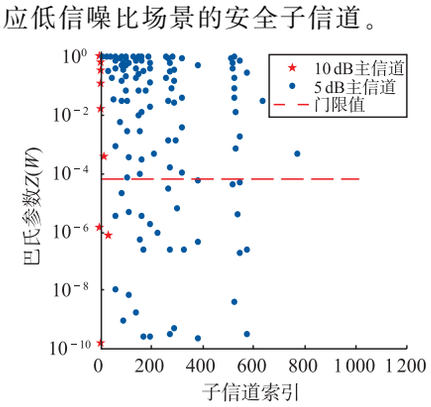

图 8　高、低信噪比场景下子信道巴氏参数对比图

从图 9～10 中可以看出，在低信噪比场景下采用本方法，当窃听方信噪比退化幅度达到 1.5 dB 时，窃听方的误码率逼近 0.5，误码块率逼近于 1。相较于采取安全极化码时的误码率和误码块率可以看出本方法在低信噪比场景下相等的窃听信道信噪比退化幅度时表现出了更好的安全性。从整体上来看，采用本方法时伴随有限域逐渐增大，窃听方的误码率和误码块率逐渐升高。

从以上仿真结果来看，本方法无论是在高、低信噪比场景下对比传统安全极化码都可以在较小的窃听信道退化幅度下，使窃听方译码结果的误码率 ber_E 趋近于 0.5 和误码块率 $bler_E$ 趋近于 1。当窃听方信噪比不变时，伴随着有限域 GF(p)中 p 增大，窃听方的两项指标都会增高，表明窃听效果在恶化。

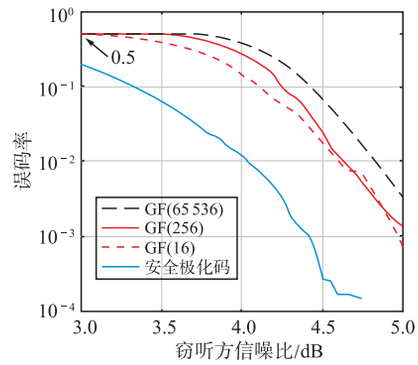

图 9　低信噪比场景下窃听方误码率对比图

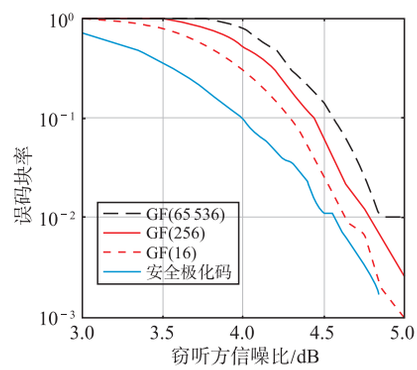

图 10　低信噪比场景下窃听方误码块率对比图

5　总结与展望

本文将网络编码与安全极化码技术进行结合，利用极化码的特点，从信道编码的角度提升网络编码系数的安全性；利用网络编码的特点，从而发挥网络编码系数差错的扩散性，使得窃听方有限的网络编码系数误比特能够更大幅度地影响网络编码译码的正确率，进一步降低窃听方的监听能力。

从开销角度来看，相比较于传统安全极化码方法，本方法需要为网络编码系数分配比特信道，需要在收发方进行网络编码译码的运算从而产生一定的通信时延。在存在中继的网络编码通信系统中，可以发挥网络编码技术的吞吐量优势，降低传输时延差距。对比传统密码学加密方法，本方法的计算复杂度和传输时延具有一定的优势。

从抗窃听性能的角度来看，在不享受网络编码分集增益优势的情况下，通过网络编码与安全极化码的级联，本方法可以在高信噪比条件下获得较好的抗窃听性能。如果在实际应用过程享受网络编码分集优势，窃听方的信道退化会更加明显，理论上可以取得更好的抗窃听效果。

实际通信系统面临的威胁更加复杂，除窃听攻击外，以污染攻击为代表的其他攻击方式也对系统的安全可靠性造成严重威胁，等待结合其他新兴技术进行化解。

参考文献

[1] 曹阳，李岳，李小红. 无线光通信中极化码构造方法研究[J]. 光学学报，2020，40(21)：25-31.

[2] 翟玉爽，冯海泓，李记龙. 极化码在 OFDM 水声通信中的应用研究[J]. 声学技术，2021，40(1)：29-38.

[3] ARIKAN E. Channel Polarization：A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels[J]. IEEE Communications Letters，2009，13(7)：519-521.

[4] HOF E，SHAMAI S. Secrecy-Achieving Polar-coding [C]//IEEE Information Theory Workshop. Dublin，Ireland：IEEE，2010：262-263.

[5] 楼泽斌. 高斯窃听信道下基于极化码的安全信道编码技术研究[D]. 杭州：浙江大学，2018.

[6] 张胜军，钟州，金梁，等. 基于安全极化码的密钥协商方法[J]. 电子与信息学报，2019，41(6)：1413-1419.

[7] LI Z，HAN Y，LI Y. Application of Polar Code-Based Scheme in Cloud Secure Storage[C]// The 6th International Conference of Pioneering Computer Scientists，Engineers and Educators (ICPCSEE 2020) Part I. Taiyuan，China：[s. n.]，2020：160-162.

[8] SUN C，FEI Z，LI B，et al. Secure Transmission in Downlink Non-Orthogonal Multiple Access Based on Polar Codes[J]. China Communications，2021，18(9)：221-235.

[9] 杨双千. 协作通信中基于系统极化码的网络编码研究[D]. 成都：西南交通大学，2019.

[10] 刘锦. 面向双向中继通信的 Polar 码与物理层网络编码联合设计[D]. 哈尔滨：哈尔滨工业大学，2020.

[11] 夏禹. 移动自组网中基于网络编码的可靠安全通信算法设计与实现[D]. 南京：东南大学，2020.

[12] CHUNG S Y，RICHARDSON T J，URBANKE R. Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation[J]. IEEE Transactions on Information Theory，2001 47(2)：657-670.

[13] CROFT J，PATWARI N，KASERA S K. Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors [C]//Proceedings of the ACM/IEEE International Conference on Information Processing in Sensor Networks. New York，USA：IEEE，2010：1124-1129.

[14] 钱萍. 基于网络编码的 WSN 隐私保护研究[J]. 南京邮电大学学报：自然科学版，2015，35(5)：41-47.

[15] JIAO L，WANG N，WANG P，et al. Physical Layer Key Generation in 5G Wireless Networks[J]. IEEE Wireless Communications，2019，26(5)：48-54.

[16] 于永润. 极化码编译码技术研究[D]. 南京：东南大学，2019.

[17] 李业，高锐锋. 基于随机线性网络编码和 UDP 的可靠低时延传输方法[J]. 南通大学学报：自然科学版，2019，18(4)：16-23.

[18] TAL I，VARDY A. List Decoding of Polar Codes [J]. IEEE Transactions on Information Theory，2015，61(5)：2213-2226.

[19] 朱巍，梁俊，肖楠，等. 随机网络编码的卫星时隙 ALOHA 碰撞重传策略[J]. 空军工程大学学报：自然科学版，2015，16(6)：17-21.

[20] SALEH M D R，TAVAKOLI H. Achieving Secure Communication over Wiretap Channels Using the Error Exponent of the Polar Code[J]. Engineering Letters，2022，30 (1)：375-379.

（编辑：徐楠楠）