文章编号：1003－1251(2025)05－0037－07

基于脉冲位置调制的帧变换差分混沌移位键控系统

隋 涛[a],韩佳依[b],杜智豪[b],于其豪[b]

(沈阳理工大学 a. 自动化与电气工程学院,b. 信息科学与工程学院,沈阳 110159)

摘 要：为解决传统差分混沌移位键控(differential chaotic shift keying,DCSK)系统安全性较差及误码性能受限的问题,提出一种结合脉冲位置调制与动态帧变换技术的DCSK(frame-transform DCSK system based on pulse position modulation,FT-PPM-DCSK)系统,实现安全性与误码性能的协同优化。通过推导系统在加性高斯白噪声(additive white Gaussian noise,AWGN)信道下的误比特率(BER)表达式,基于蒙特卡洛仿真验证其性能。实验结果表明,与基准DCSK系统相比,FT-PPM-DCSK系统提高了误码性能且具有更高的安全性。

关 键 词：差分混沌移位键控;脉冲位置调制;帧变换;误码性能

中图分类号：TN918 **文献标志码**：A **DOI**:10.3969/j.issn.1003－1251.2025.05.006

Frame-transform Differential Chaotic Shift Keying System Based on Pulse Position Modulation

SUI Tao,HAN Jiayi,DU Zhihao,YU Qihao

(Shenyang Ligong University,Shenyang 110159,China)

Abstract: To solve the problems of poor security and limited bit error performance of traditional differential chaotic shift keying system(DCSK),a differential chaotic shift keying system combining pulse position modulation and dynamic frame transform technology(FT-PPM-DCSK) is proposed. Based on the hybrid modulation strategy of frame transformation,the system uses pulse position modulation(PPM) to modulate part of the information bits to achieve the collaborative optimization of security and bit error performance. The bit error rate(BER) expression of the system in additive white Gaussian noise(AWGN) channel is derived,and its performance is verified by Monte Carlo simulation. The experimental results show that,compared with the benchmark DCSK system,the FT-PPM-DCSK system improves the BER performance and has higher security.

Key words: differential chaotic shift keying;pulse position modulation;frame transform;bit error rate performance

随着通信技术的快速发展,混沌信号凭借其初值敏感性和长期不可预测性的特征,在提升通信系统安全性方面展现出独特优势,已成为扩频通信领域的重要研究方向[1－3]。差分混沌移位键控(differential chaotic shift keying,DCSK)系统由于其硬件复杂度低、抗多径干扰能力强等优点,成为研究的热点[4－5]。DCSK使用传输参考(transmitted-reference,T-R)结构将每个位的持续时间划分为参考时隙与信息时隙[6],利用混沌信号自相关特性实现非相干解调。然而,传统混沌调制

收稿日期：2025－03－20

基金项目：辽宁省教育厅高等学校基本科研项目(JYTMS20230199)

作者简介：隋涛(1978—),男,副教授,博士。

方案在应对现代通信对高带宽和大容量数据传输的需求时,暴露出单位符号能量利用率不足导致传输速率受限、固定帧结构造成安全隐患、时隙分配刚性制约频谱效率三个问题。

为此,学者们做了大量研究工作,提出了多个改进的 DCSK 通信方案。在提升系统传输速率方面,利用混沌信号的准正交特性,分别提出了置换索引 DCSK(PI-DCSK)[7] 和置换码索引 DCSK(CCI-DCSK)[8],以通过预定义的置换来发送额外的信息位。正交 DCSK(QCSK)[9] 通过在信息承载时隙中添加两个正交混沌序列携带两个信息比特。文献[10]设计了一种基于脉冲位置调制的 DCSK(PPM-DCSK),将额外的信息比特映射到相应的位置索引,以获得更好的误码率性能。文献[11]提出了一种带索引调制的双模式 DCSK 系统(DM-DCSK-IM),调制比特由一对可区分的调制模式星座承载。为了进一步提高数据速率,文献[12]在下行链路多用户传输中开发了叠加编码的 PPM-DCSK。该方案根据脉冲的位置区分用户并传输额外的比特。在提升系统安全性方面,文献[13]给出了一种时间反转参考信号调制 DCSK(TR-RM-DCSK)系统方案,将参考信号进行时间反转,消除了同一帧时隙信号间的相关性。基于上述技术演进,本文提出一种结合脉冲位置调制与动态帧变换技术的 DCSK(frame-transform DCSK system based on pulse position modulation, FT-PPM-DCSK)系统。该方案引入的动态帧变换技术提高了信息传输的安全性,同时也具备 PPM 调制策略较高传输速率的优点。

本文的主要研究内容如下:

1)提出一种结合脉冲位置调制与动态帧变换技术的 DCSK 系统,以提升安全性并优化误码性能;

2)利用高斯近似(Gaussian approximation, GA)[14]法建立 FT-PPM-DCSK 系统在 AWGN 信道下的理论误码率模型,推导误比特率(BER)表达式;

3)通过蒙特卡洛仿真[15]验证 FT-PPM-DCSK 系统在复杂信道条件下的鲁棒性;

4)通过对比 DCSK、TR-RM-DCSK 等基准方案,分析 FT-PPM-DCSK 系统在不同信道环境下的性能;

5)在 FT-PPM-DCSK 系统中引入混沌敏感性、排列组合复杂度和 m 序列不可预测性三重机制,以拓展密钥空间,克服 PPM-DCSK 因调制参数的精度受限而存在的安全隐患。

1 系统基本原理

1.1 系统帧结构

FT-PPM-DCSK 系统的信号结构如图 1 所示。该系统的时间帧由多个时隙单元组成,每个时隙包含参考信号和信息信号两个部分。

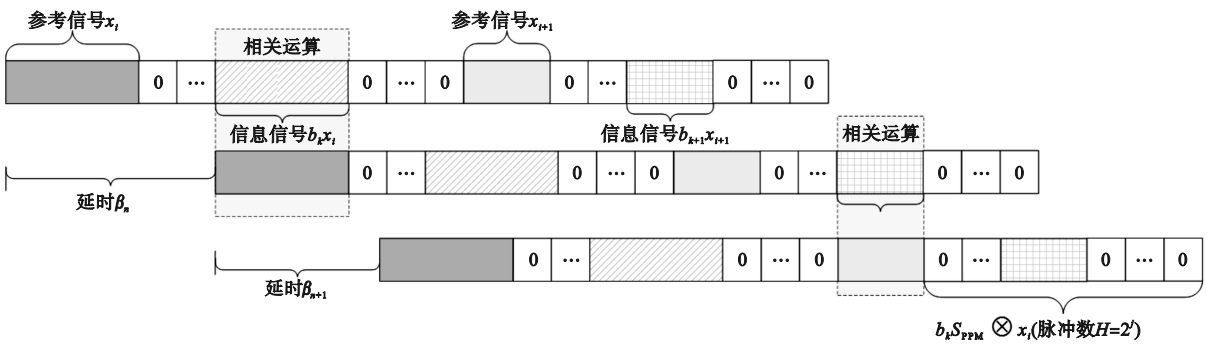

图 1 FT-PPM-DCSK 信号结构图

Fig. 1 FT-PPM-DCSK signal structure diagram

参考信号 x_i 由混沌信号发生器生成,为接收端解调提供相位基准。信息信号由两部分构成:一部分采用 PPM 调制,通过脉冲在时间轴上的位置对比特信息进行编码;另一部分则通过混沌信号的极性变化实现调制。每个时间帧的长度及时隙分配采用帧变换技术进行动态调整,以降低相邻比特间的相关性。第 k 帧的传输信号 $s_{i,k}$ 表示为

$$s_{i,k}=\begin{cases} x_i, & i=2\beta_1(k-1)+1,\cdots, 2\beta_n(k-1)+n \\ b_k S_{\mathrm{PPM}}\otimes x_{i-\beta_n}, & i=2\beta_1(k-1)+\beta_1+1,\cdots, 2\beta_n(k-1)+\beta_n+n \end{cases} \tag{1}$$

$$S_{\mathrm{PPM}}=[0,0,\cdots,1_{e_k},\cdots,0]_{1\times H}(H=2^j) \tag{2}$$

式中:$b_k\in\{-1,1\}$,为信息位,信息位在 PPM 帧中

的一个位置上传输,该位置通过映射位确定;⊗为克罗内克算子;$x_{i-\beta_n}$表示由混沌发生器产生长度为β_n的混沌序列经过延迟β_n单位后形成的混沌序列;n表示系统中所使用的不同延迟的数量;S_{PPM}为PPM信号;H表示一个信息承载信号内的总时隙量;j表示映射到PPM索引调制符号的位置的位数;e_k为由映射比特转换得到的一个位置索引调制符号,其中1_{e_k}表示S_{PPM}的第e_k个位置为1。

1.2　发射机结构

FT-PPM-DCSK发射机首先通过可变换模组与延时模块对混沌信号x_i施加动态延迟β_n并复制H倍,随后,根据待传输的信息,将其映射至对应的脉冲位置,其他脉冲位置信号则为空。在包含信息的脉冲位上,根据传输比特值为"0"或者"1",分别采用"－"或者"＋"来表示,从而作为DCSK解调判决的依据。最终,通过混沌信号、脉冲位置调制及符号映射的协同作用,生成调制后的输出信号$S_{i,k}$,并将其发送至通信信道。其发射机结构如图2所示。

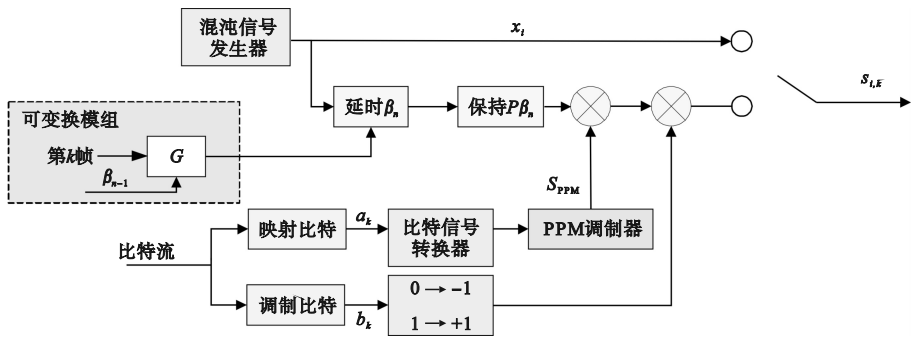

图2　FT-PPM-DCSK发射机结构

Fig. 2　FT-PPM-DCSK transmitter structure

发射机总发射比特数为$j+1$,PPM部分包含j位比特信号a_k,另外1比特信号由DCSK调制提供,符号持续时间为$(2^j+1)\beta_n$。本文选取差分跳频通信中常用的G函数算法充当此处的可变换模块,其数学表示式为

$$\beta_n = G(\beta_{n-1}, X_n) \tag{3}$$

式中:β_{n-1}为上一时隙的延时长度;X_n为携带的信息。

1.3　接收机结构

FT-PPM-DCSK接收机结构如图3所示。该接收机不仅需要对DCSK信号的调制比特进行解调,还需识别PPM调制的脉冲索引位置,以准确恢复传输信息。

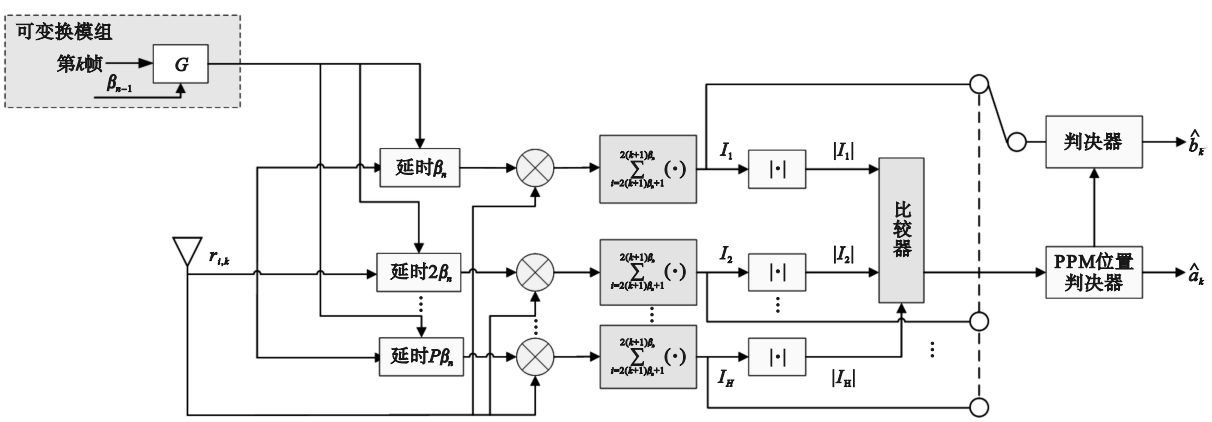

图3　FT-PPM-DCSK接收机结构

Fig. 3　FT-PPM-DCSK receiver structure

假设接收机首先接收到信号已受到多径瑞利衰落信道的影响,则接收信号$r_{i,k}$可以表示为[16]

$$r_{i,k} = \sum_{l=1}^{L} \alpha_l \delta(t-\tau_l) \otimes s_{i,k} + n_i \tag{4}$$

式中:L表示信道数量;α_l和τ_l分别表示第l条信道的传播增益系数和路径时延,当通道数为1且$\alpha_l=1$,$\tau_l=0$时,多径瑞利衰落信道可以近似为AWGN信道;n_i表示均值为0、方差为N_0的加性

高斯白噪声。

接收机首先接收到输入信号 $r_{i,k}$，并对其进行从 β_n、$2\beta_n$ 到 $H\beta_n$ 的多径延迟处理。随后，利用相关器对延时后的参考信号与接收到的数据信号进行相关运算，计算 H 个分支的相关输出 $I_1, I_2, \cdots, I_H$，并将其绝对值 $|I_1|, |I_2|, \cdots, |I_H|$ 输入至比较器中。最大绝对值对应的元素即为用于映射比特恢复的元素 $\hat{a}_k$。通过确定该元素的位置，并采用十进制到二进制的映射恢复 PPM 调制比特，同时依据该元素的极性判定 DCSK 调制比特 $\hat{b}_k$，实现完整的信息恢复。

2 系统性能分析

2.1 系统总误码率分析

当 H 个分支中的第 m 路的值与 e_k 在 S_{PPM} 的位置索引相等时，其决策变量 I_m 可以表示为

$$I_m = \sum_{i=1}^{\beta_n} \left(\sum_{l=1}^{L} \alpha_l x_i + n_i \right) \left(\sum_{l=1}^{L} \alpha_l b_k x_i + n_{i-\beta_n} \right) \quad (5)$$

类似地，当 H 个分支中的第 m 路的值与 e_k 在 S_{PPM} 的位置索引不相等时，其决策变量 I'_m 可以表示为

$$I'_m = \sum_{i=1}^{\beta_n} \sum_{l=1}^{L} \alpha_l x_i n_{i-\beta_n} + \sum_{i=1}^{\beta_n} n_i n_{i-\beta_n} \quad (6)$$

系统总误码率由调制比特的误码率 P_{em} 和映射比特的误码率 P_{ecim} 共同决定，其表达式为

$$P_{\mathrm{sys}} = \frac{j}{j+1} P_{\mathrm{ecim}} + \frac{1}{j+1} P_{\mathrm{em}} \quad (7)$$

正确的调制比特估计取决于位置检测与解调过程的准确性。可能导致误差的两种情况如下：第一种情况为信息序列的位置检测正确，但调制比特解调过程中发生错误；第二种情况则为位置检测错误。在此情况下，调制比特被正确检测的概率为 0.5。因此，系统的总调制比特的误码率 P_{em} 计算表达式为

$$P_{\mathrm{em}} = P_{\mathrm{e}}(1 - P_{\mathrm{ed}}) + 0.5 P_{\mathrm{ed}} \quad (8)$$

式中 P_{e} 和 P_{ed} 分别表示系统帧变换部分及 PPM 检测部分的误码率。

2.2 P_{e} 的推导

由于帧变换使得每个相邻的时隙长度不同，故使用平均半扩频因子来计算，其推导过程如下。

帧变换部分在第 k 个符号持续时间结束时的判决变量 Z_k 为

$$Z_k = \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} \left(b_k x_i^2 - \beta_n + b_k x_{i-\beta_n} n_i + x_i n_i + n_i n_{i-\beta_n} \right) \quad (9)$$

第 k 位信息比特 $b_k = +1$ 的决策变量 Z_k 的平均值为

$$E\{Z_k \mid (b_k = +1)\} = E\left\{ \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} (b_k x_i^2 - \beta_n) \right\} = \beta_n P_{\mathrm{s}} \quad (10)$$

式中：$E\{\cdot\}$ 为期望算子；$P_{\mathrm{s}} = E\{x_{i-\beta_n}^2\}$，表示混沌序列的均方值。

第 k 位信息比特 $b_k = +1$ 的决策变量 Z_k 的方差为

$$\begin{aligned} Var\{Z_k \mid (b_k = +1)\} = {} & Var\left\{ \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} (x_{i-\beta_n}^2) \right\} + \\ & Var\left\{ \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} (x_{i-\beta_n} n_i) \right\} + Var\left\{ \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} (x_{i-\beta_n} n_{i-\beta_n}) \right\} + \\ & Var\left\{ \sum_{i=2\beta_n(k-1)+n}^{2\beta_n(k-1)+\beta_n} (n_i n_{i-\beta_n}) \right\} \end{aligned} \quad (11)$$

式中 $Var\{\cdot\}$ 为方差算子。将式(11)求和整理可得

$$Var\{Z_k \mid (b_k = +1)\} = \overline{\beta}_n \Lambda + \overline{\beta}_n N_0 P_{\mathrm{s}} + \overline{\beta}_n \frac{N_0^2}{4} \quad (12)$$

其中 $\Lambda = Var\{x_{i-\beta_n}^2\}$，因此 P_{e} 可表示为

$$\begin{aligned} P_{\mathrm{e}} &= \frac{1}{2} \mathrm{erfc}\left[\left(\frac{E[Z_k \mid (b_k = +1)]}{\sqrt{2 Var[Z_k \mid (b_k = +1)]}} \right) \right] \\ &= \frac{1}{2} \mathrm{erfc}\left[\left(\frac{2\psi}{\overline{\beta}_n} + \frac{2N_0}{\overline{\beta}_n P_{\mathrm{s}}} + \frac{N_0^2}{2\overline{\beta}_n P_{\mathrm{s}}^2} \right) - \frac{1}{2} \right] \end{aligned} \quad (13)$$

式中：$\mathrm{erfc}(\cdot)$ 表示互补误差函数；$\psi = Var[x_k^2] / E^2[x_k^2]$。$\Lambda$ 与 P_{s} 取决于使用的混沌序列的特性。

2.3 P_{ed} 的推导

映射比特的误码率 P_{ecim} 的计算表达式为

$$P_{\mathrm{ecim}} = (Q/j) P_{\mathrm{ed}} \quad (14)$$

$$Q = \sum_{g=1}^{j} g \frac{\binom{j}{g}}{H-1} \quad (15)$$

式中：Q 为误差数量的期望；$\binom{j}{g} = j!/g!(j-g)!$，表示在 j 比特中选择 g 个错误比特的可能情况数量。从上述公式可以看出，FT-PPM-DCSK 系统的总误码概率由两部分组成，其中帧变换部分的贡献相对较小，PPM 部分占据主导地位，是其误码率较 PPM-DCSK 未得到改善的关键原因。

假设调制比特和 PPM 的位置索引都被成功传输，则 I_m 和 I'_m 的平均值 μ_1、μ_2 和方差 σ_1^2、σ_2^2 分别为

$$\mu_1 = E\{I_m\} = \frac{\sum_{l=1}^{L}\alpha_l^2 E_s}{2},\ \mu_2 = E\{I'_m\} = 0 \quad (16)$$

$$\sigma_1^2 = \sum_{l=1}^{L} Var\{I_m\} = \frac{\sum_{l=1}^{L}\alpha_l^2 E_s N_0}{2} + \frac{N_0^2\beta_n}{4}, \sigma_2^2 = Var\{I'_m\} = \frac{\sum_{l=1}^{L}\alpha_l^2 E_s N_0}{4} + \frac{N_0^2\beta_n}{4} = E_s N_0 \underbrace{\left(\frac{\sum_{l=1}^{L}\alpha_l^2}{4} + \frac{\beta_n}{4r_s}\right)}_{\lambda} \quad (17)$$

式中:$E_s = 2\beta_n E\{x_i^2\}$,表示 FT-PPM-DCSK 的符号能量;$r_s = \sum_{l=1}^{L}\alpha_l^2 E_s/N_0$,表示信噪比。随机变量$|I_m|$和$|I'_m|$遵循相同的折叠正态分布,因此$|I_m|$的概率密度函数和$|I'_m|$的累积分布函数分别计算如下。

$$f_{|I_m|}(y) = \frac{1}{\sqrt{2\pi\sigma^2_{|I_m|}}}\left[e^{-\frac{(y-\mu_{|I_m|})^2}{2\sigma^2_{|I_m|}}} + e^{-\frac{(y+\mu_{|I_m|})^2}{2\sigma^2_{|I_m|}}}\right] \quad (18)$$

$$F_{|I'_m|}(y) = \mathrm{erf}\left(\frac{y}{\sqrt{2\sigma_2^2}}\right) \quad (19)$$

式中:erf(·)表示误差函数;$\mu_{|I_m|}$和$\sigma^2_{|I_m|}$表示$|I_m|$的均值和方差,表达式分别为

$$\mu_{|I_m|} = \sqrt{\frac{2\sigma_1^2}{\pi}}e^{-\frac{\mu_1^2}{2\sigma_1^2}} - \mu_1\mathrm{erf}\left(\frac{-\mu_1}{\sqrt{2\sigma_1^2}}\right) = \sqrt{E_s N_0}\gamma \quad (20)$$

其中

$$\gamma = \sqrt{\frac{1}{2\pi} + \frac{R}{4\pi r_s}}e^{\left(-\frac{1}{\frac{4}{r_s}+\frac{2\beta_n}{r_s^2}}\right)} - \frac{\sqrt{r_s}}{2}\mathrm{erf}\left(-\sqrt{\frac{1}{\frac{4}{r_s}+\frac{2\beta_n}{r_s^2}}}\right) \quad (21)$$

$$\sigma^2_{|I_m|} = \mu_1^2 + \sigma_1^2 - \mu^2_{|I_m|} = E_s N_0 \underbrace{\left(\frac{r_s}{4} + \frac{1}{2} + \frac{\beta_n}{4r_s} - \gamma^2\right)}_{\rho} \quad (22)$$

定义目标位置的检测统计量为 Y,其余 $H-1$ 个非目标位置上的最大干扰统计量为 $X_1 = \max\{|I_m|\}$,$m = 1,2,\cdots,H-1$,PPM 检测错误概率可以通过目标统计量小于干扰最大值的概率计算得到,即

$$P_{ed} = 1 - P_r\{Y \geqslant X\} = \int_0^\infty [1 - P_r\{Y \geqslant X\}]f_{|I_m|}(y)\mathrm{d}y = \frac{1}{\sqrt{2\pi\sigma^2_{|I_m|}}}\int_0^\infty \left[1 - \left[\mathrm{erf}\left(\frac{y}{\sqrt{2\sigma_2^2}}\right)\right]^{H-1}\right]\times \left[e^{\frac{(y-\mu_{|I_m|})^2}{2\sigma^2_{|I_m|}}} + e^{-\frac{(y+\mu_{|I_m|})^2}{2\sigma^2_{|I_m|}}}\right]\mathrm{d}y \quad (23)$$

式中 $P_r\{\cdot\}$ 表示概率运算。假设 $\mu = \frac{y}{\sqrt{E_s N_0}}$,则位置检测错误概率为

$$P_{ed} = \frac{1}{\sqrt{2\pi\rho}}\int_0^\infty \left[1 - \left[\mathrm{erf}\left(\frac{\mu}{\sqrt{2\lambda}}\right)\right]^{H-1}\right]\times \left\{e^{-\frac{(y-\gamma)^2}{2\rho}}e^{-\frac{(y+\gamma)^2}{2\rho}}\right\}\mathrm{d}\mu \quad (24)$$

将式(24)代入式(14)可得映射比特的误码率;将式(8)和式(14)代入式(7)可得 PPM-FT-DCSK 的瞬时误码率。

3　实验与仿真分析

3.1　仿真与理论误码率对比

为验证 FT-PPM-DCSK 系统在 AWGN 信道中的误码率模型准确性,本节通过理论推导与仿真实验相结合的方法,对比分析其理论计算与仿真结果的吻合度。

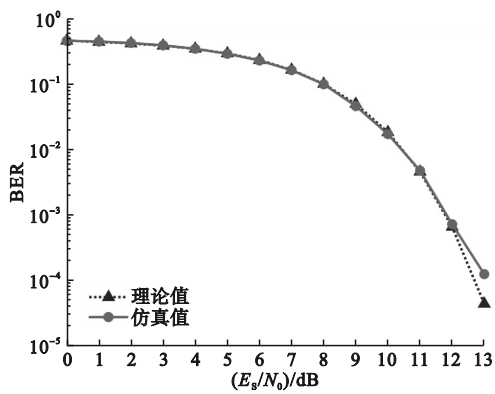

图 4　FT-PPM-DCSK 系统在 AWGN 信道中的理论误码率与仿真误码率比较

Fig. 4　Comparison between theoretical and simulated BER of FT-PPM-DCSK system in AWGN channel

图 4 表明,FT-PPM-DCSK 系统的理论 BER 曲线与仿真结果高度一致,验证了所推导误码率模型的准确性。这一结果为该技术在更复杂信道环境下的性能研究提供了理论支撑,同时为系统参数优化及实际应用奠定了分析基础。

3.2　不同混沌系统误码性能比较

为了探究 FT-PPM-DCSK、PPM-DCSK、TR-RM-DCSK 和 DCSK 四种系统在不同信噪比(r_s)条件下的误码性能,实验采用初值为 0.4 的改进型 Logistic 映射作为混沌信号,并通过蒙特卡洛仿真进行实验。仿真结果如图 5 所示。

结果表明,FT-PPM-DCSK 系统在各个信噪比

范围内的误码率性能均优于 DCSK 和 TR-RM-DCSK,表现出更优的抗噪性能。同时,与 PPM-DCSK 相比,FT-PPM-DCSK 误码率并未显著增加,表明其在保持 PPM-DCSK 系统可靠性的前提下,实现了更优的性能优化。

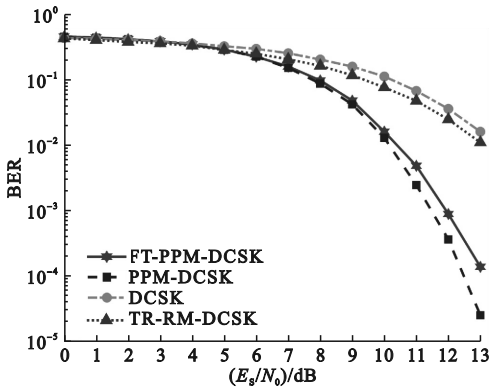

图 5 不同混沌系统误码率对比

Fig. 5 BER comparison of different chaotic systems

3.3 不同信道下的误码性能比较

图 6 展示了 FT-PPM-DCSK 与 TR-RM-DCSK 在 AWGN、Rician 和 Rayleigh 信道条件下的误码率随信噪比的变化趋势。

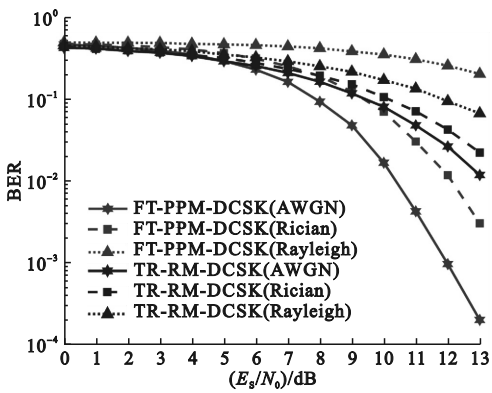

图 6 FT-PPM-DCSK 与 TR-RM-DCSK 在不同信道下误码率对比

Fig. 6 BER comparison between FT-PPM-DCSK and TR-RM-DCSK under different channels

从图中看出,在 AWGN 和 Rician 信道中,FT-PPM-DCSK 方案的误码率明显优于 TR-RM-DCSK,尤其是在高信噪比区域,性能优势更加突出。这表明其在抗噪声和抗衰落方面具有更好的稳健性。然而,在 Rayleigh 信道环境下,TR-RM-DCSK 的性能相对较优,这主要是由于 Rayleigh 信道的深度衰落特性对 PPM 调制的影响较大,使得 FT-PPM-DCSK 在低信噪比条件下受到较大性能损失。尽管如此,FT-PPM-DCSK 在 AWGN 和 Rician 信道中的显著增益仍表明其在多种实际无线通信环境中具备更广泛的应用潜力。

3.4 不同映射位数的误码性能比较

图 7 展示了 FT-PPM-DCSK 系统在不同映射因子 j 条件下的误码率随信噪比变化的趋势。

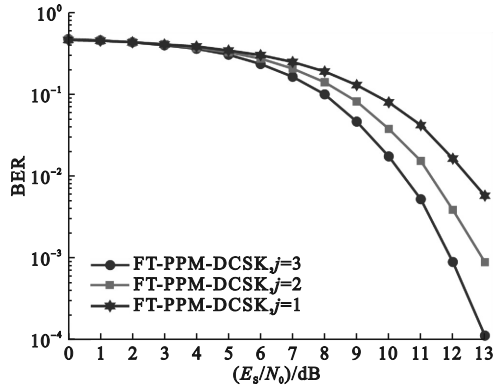

图 7 FT-PPM-DCSK 在不同 j 下的误码率对比

Fig. 7 BER comparison of FT-PPM-DCSK under different j values

结果表明,随着映射因子 j 的增加,系统的误码率逐步降低,表明更高的 j 值可以有效提升系统的抗噪声能力。然而,尽管较高的 j 提供了更优的误码率性能,但同时也会带来额外的带宽消耗和系统复杂度的增加。因此,在实际应用中,需要权衡误码率性能与资源利用效率,以优化系统设计。

3.5 不同系统的安全性比较

密钥空间是密码学中衡量系统安全性的核心指标,定义为所有可能密钥组合的数量。密钥空间越大,攻击者需尝试的密钥数量越多,破解时间指数级增长,以抵抗暴力破解。大密钥空间确保密文与密钥之间无统计相关性,无法通过模式推断破解,以抵抗统计攻击。固定扩频因子或重复使用的混沌序列会导致自相关性、频域特征等密文统计特征泄露,攻击者可通过模式匹配缩小密钥搜索范围。

实验中,PPM-DCSK 与 FT-PPM-DCSK 使用相同的混沌序列与调制参数并传输相同的比特数,故二者调制参数空间 K_ξ 相同,则 PPM-DCSK 密钥空间计算表达式为

$$K_{\text{PPM-DCSK}} = K_\xi \times K_{\text{固定SF}} = M \times 1 = M \quad (25)$$

FT-PPM-DCSK 密钥空间由调制参数、m 序列生成机制及 SF 平均排列数三个部分组成。其中,m 序列通过线性反馈移位寄存器(LFSR)生成,长度设定为 10 位,其密钥空间由初始状态决定,在排除全零状态后共计 $K_{m\text{序列}} = 2^{10} - 1 = 1\,023$ 种可能,近似为 10^3。为消除单组实验的偶然性,在 10

组异构通信场景下开展测试,精确统计各实验组内唯一 SF 排列的数量 N_v。基于各实验组间 SF 排列数相互独立且等权分布的假设,计算其排列数的对数并取算术平均,再转换为实际值,该多场景 SF 跳变动态参数表如表 1 所示。系统自相关性、功率谱密度等关键统计特征随 SF 变化而随机变化,使得攻击方难以基于历史观测数据构建有效的统计推断模型。

表 1　多场景 SF 跳变动态参数表

Table 1　Multi scenario SF jump dynamic parameters

组别	$\log_{10}(N_v!)$	$N_v!$（科学计数法）
第一组	25.50	3.16×10^{25}
第二组	24.70	5.04×10^{24}
第三组	26.43	2.68×10^{26}
第四组	23.79	6.20×10^{23}
第五组	22.41	2.58×10^{22}
第六组	24.70	5.04×10^{24}
第七组	25.50	3.16×10^{25}
第八组	27.48	3.05×10^{27}
第九组	23.79	6.20×10^{23}
第十组	25.50	3.16×10^{25}

故 FT-PPM-DCSK 的密钥空间计算表达式为

$$K_{\text{FT-PPM-DCSK}} = K_{\xi}\times K_{m\text{序列}}\times K_{\text{SF平均排列数}} = 9.55\times10^{27}M \tag{26}$$

安全性优势 K' 为

$$K' = \frac{K_{\text{FT-PPM-DCSK}}}{K_{\text{PPM-DCSK}}} = 9.55\times10^{27} \tag{27}$$

FT-PPM-DCSK 系统通过混沌敏感性、排列组合复杂度和 m 序列不可预测性三重机制,即使攻击者获取其中部分密钥分量,也无法推断剩余分量或历史/未来密钥,将密钥空间从 M 提升至 $10^{27}M$,弥补了 PPM-DCSK 因调制参数的精度不足导致的安全缺陷。

4　结论

本文提出的 FT-PPM-DCSK 系统通过融合 PPM 调制的高能效特性与动态帧变换技术的灵活性,提升了安全性并优化了误码性能。理论推导与仿真实验表明,该系统在 AWGN 和 Rician 信道中较基准 DCSK 误码率降低,并通过混沌敏感性、动态参数跳变和 m 序列生成器的三重加密机制,将密钥空间显著扩展,有效抵御暴力破解与统计攻击。尽管在瑞利信道低信噪比条件下性能受限,但其在物联网抗干扰通信与 6G 物理层安全增强等领域展现出广阔应用潜力,未来研究可着重于优化 PPM 映射策略与自适应帧变换技术的结合,利用先进的信道编码和机器学习方法,进一步突破性能瓶颈。

参考文献(References):

[1] FANG Y,PAN Y C,MA H,et al. A novel DCSK-based linear frequency modulation waveform design for joint radar and communication systems[J]. IEEE Transactions on Green Communications and Networking,2025,9(1):354 – 366.

[2] WANG Q Q,WANG W D,LONG B Q,et al. Adaptive parallel DCSK with code index modulation for implantable sensor networks[C]//2024 IEEE 10th International Symposium on Microwave,Antenna,Propagation and EMC Technologies for Wireless Communications (MAPE). Guangzhou, China: IEEE,2024:1 – 4.

[3] KANG P,ZHU Z Q,LIN Z J,et al. Design of chaotic-based PPM-PI-DCSK modulation for wireless communications[J]. IEEE Wireless Communications Letters, 2023, 12 (10): 1662 – 1666.

[4] ZHANG G,CHEN X B,HU Y N. Singular value decomposition optimizes multi-level orthogonal code index modulation DCSK system[J]. IEEE Communications Letters, 2024, 28 (12):2874 – 2878.

[5] CAI X M,XU W K,WANG L,et al. Multicarrier M-ary orthogonal chaotic vector shift keying with index modulation for high data rate transmission[J]. IEEE Transactions on Communications,2020,68(2):974 – 986.

[6] CAI X M,XU W K,MIAO M Y,et al. Design and performance analysis of a new M-ary differential chaos shift keying with index modulation[J]. IEEE Transactions on Wireless Communications,2020,19(2):846 – 858.

[7] HERCEG M,KADDOUM G,VRANJEŠ D,et al. Permutation index DCSK modulation technique for secure multiuser high-data-rate communication systems[J]. IEEE Transactions on Vehicular Technology,2018,67(4):2997 – 3011.

[8] HERCEG M,VRANJEŠ D,KADDOUM G,et al. Commutation code index DCSK modulation technique for high-data-rate communication systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs,2018,65(12):1954 – 1958.

[9] GALIAS Z,MAGGIO G M. Quadrature chaos-shift keying: theory and performance analysis[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,2001,48(12):1510 – 1519.

[10] MIAO M Y,WANG L,KATZ M,et al. Hybrid modulation scheme combining PPM with differential chaos shift keying modulation[J]. IEEE Wireless Communications Letters, 8 (2):340 – 343.

[11] CAI X M,XU W K,HONG S H,et al. Dual-mode differential chaos shift keying with index modulation[J]. IEEE Transactions on Communications,2019,67(9):6099 – 6111.

[12] MA H,CAI G F,FANG Y,et al. Design of a superposition coding PPM-DCSK system for downlink multi-user transmission[J]. IEEE Transactions on Vehicular Technology,2020, 69(2):1666 – 1678.

(下转第 58 页)