文章编号:1009-3087(2016)03-0142-06 DOI:10.15961/j.jsuese.2016.03.019

采用4-WFRFT和人工噪声的变换域通信物理层安全传输

王 舒,达新宇,褚振勇,朱丽莉
(空军工程大学 信息与导航学院,陕西 西安 710077)

摘 要:为了提高变换域通信(TDCS)信号的物理层安全性,提出一种基于4项加权分数傅里叶变换(4-WFRFT)和人工噪声的TDCS信号加密方式。利用4-WFRFT代替传统TDCS中的DFT/IDFT,改变了TDCS信号的空间分布,在保持原系统复杂度的同时增加了TDCS信号的抗截获性。在此基础上,使用人工噪声进一步增强系统的安全性,并推导了非法用户理论误码率以及系统保密容量。仿真结果表明,无论是全频谱还是频谱失配情况下,当参数α在[0,0.8)或(1.7,4]时,窃听者误码率始终保持在0.5,故无法正确解调发送信号,同时,系统保密容量为正数,有效保证了信息的安全传输。

关键词:变换域通信系统;加权分数傅里叶变换;人工噪声;物理层安全
中图分类号:TN914.42 **文献标志码**:A

Secure Transmission for TDCS Using 4-WFRFT and Noise Insertion

WANG Shu, DA Xinyu, CHU Zhenyong, ZHU Lili
(Info. and Navigation College, Air Force Eng. Univ., Xi'an 710077, China)

Abstract: In order to guarantee the physical layer security of the transform domain communication system (TDCS), a security-enhanced scheme based on 4-weighted-type fractional Fourier transform (4-WFRFT) and artificial noise insertion was proposed. Firstly, the 4-WFRFT was applied to TDCS instead of the discrete Fourier transform (DFT) and inverse discrete Fourier transform (IDFT), which maintained the system complexity while made the distribution of TDCS signals change in the complex plane. Then the artificial noise was inserted to further enhance the security. The expression of the bit error rate (BER) and the security capacity for eavesdroppper were obtained. Simulation results showed that whether with or without spectrum mismatch, the BER for eavesdropper kept 0.5 and the security capacity was positive when was in the range of [0, 0.8) or (1.7, 4] in the security-enhanced TDCS.

Key words: transform domain communication system (TDCS); 4-weighted-type fractional Fourier transform; artificial noise; physical layer security

变换域通信系统(transform domain communication system, TDCS)是在认知无线电(cognitive radio, CR)、扩频通信和变换域处理技术基础上发展而来的新技术[1],凭借其良好的抗干扰性[2]和频谱利用率的有效性[3-4],受到越来越广泛的关注。然而,由于无线信道的开放性和电磁信号传播的广播特性使TDCS对保密性及安全性的需求变得日益突出。

TDCS采用类噪声的基函数调制信息,使其具备一定的低截获(low probability of intercept, LPI)的特性,而基函数中的伪随机相位序列设计与其LPI特性密不可分。王传丹等[5]提出了采用双m序列控制基函数相位映射的方法,增强了基函数的随机性;何世彪、Sun[6-7]等分别采用了混沌序列和Golden序列,但其实质都是增强伪随机相位的随机性。由于受到系统复杂度的约束,实际应用中伪随机码序列的规模是有限的。一旦窃听者具有超强计算能力,就有可能通过快速有效的方法搜索并捕获合法通信采用的码序列,使整个系统无法保证安全通信。Mei等[8]采用了新的变换域技术即加权分数傅立叶变换(weighted-type fractional Fourier transform, WFRFT),建立了基

收稿日期:2015-06-27
基金项目:国家自然科学基金资助项目(61271250)
作者简介:王 舒(1987—),女,博士生. 研究方向:变换域通信与通信信号处理. E-mail:xss_wang@163.com

于 WFRFT 的数字通信系统框架,其分析和仿真结果表明通过参数调整的 WFRFT 信号具有很强的 LPI 性能。Fang 等[9]进一步提出了一种基于并行扩频的 WFRFT,在 WFRFT 信号的映射过程中同时利用了扩频序列的伪随机性,从而获得更好的 LPI 性能。由于无线信道的不可逆性,Goel 等[10]有意添加了人工噪声以保证物理层传输的安全。但是,文献[8-9]的研究均只针对变换域过程,并没有考虑如何应用于不同通信系统所带来的信号结构变化,文献[10]能否添加人工噪声与系统保密容量的大小有直接联系。因此,考虑如何结合 TDCS 与 WFRFT 的优势并在系统安全容量为正的前提下添加人工噪声是本文的研究重点。

基于此,作者提出了一种基于 4-WFRFT 和人工噪声的 TDCS 安全传输系统,将 4-WFRFT 与人工噪声同时应用于 TDCS 中。不同于基于 DFT/IDFT 的传统 TDCS,本文方法的基函数的设计利用了 4-WFRFT 的抗截获性,通过设计 4-WFRFT 的相关参数改变传统 TDCS 信号的空间分布,同时,在系统保密容量为正的前提下加入人工噪声进一步提高 TDCS 的安全传输性能。结合理论与仿真结果分析,定量地给出了参数 α 对系统误码性能以及保密容量的影响。

1　离散序列的 4-WFRFT

对于任意复数序列 $\boldsymbol{X}_0 = [x_0, x_1, x_2, \cdots, x_{N-1}]$,其$(\alpha, \boldsymbol{V})$ 阶的 4-WFRFT 定义为[8]:

$$\boldsymbol{Y}_0 = \boldsymbol{F}_{4W}^{\alpha,\boldsymbol{V}}[\boldsymbol{X}_0] = \omega_0^{\alpha,\boldsymbol{V}}\boldsymbol{X}_0 + \omega_0^{\alpha,\boldsymbol{V}}\boldsymbol{X}_1 + \omega_0^{\alpha,\boldsymbol{V}}\boldsymbol{X}_2 + \omega_0^{\alpha,\boldsymbol{V}}\boldsymbol{X}_3 \tag{1}$$

式中,$\boldsymbol{X}_0$、$\boldsymbol{X}_1$、$\boldsymbol{X}_2$、$\boldsymbol{X}_3$ 分别为序列 $\boldsymbol{X}_0$ 的 0 ~ 3 次 DFT。加权系数表示为:

$$\omega_l^{\alpha,\boldsymbol{V}} = \frac{1}{4}\sum_{k=0}^{3}\exp\left\{\frac{2\pi \mathrm{i}}{4}[(4m_k+1)\alpha(k+4n_k) - lk]\right\} \tag{2}$$

式中:$l = 0,1,2,3$;$\boldsymbol{V} = [\boldsymbol{MV}, \boldsymbol{NV}]$,$\boldsymbol{MV} = [m_0, m_1, m_2, m_3]$ 与 $\boldsymbol{NV} = [n_0, n_1, n_2, n_3]$ 均为整数向量;α 的周期为 4,通常取值区间为[0,4]。当 $\boldsymbol{V} = 0$ 时,式(1)只包含一个参数 α,称为单参数 4-WFRFT;当 $\boldsymbol{V} \neq 0$ 时,式(1)共包含 9 个参数,称为多参数 4-WFRFT。

对 $\boldsymbol{Y}_0$ 进行$(-\alpha, \boldsymbol{V})$ 阶的 4-WFRFT,可以还原 $\boldsymbol{X}_0$,即:

$$\boldsymbol{X}_0 = \boldsymbol{F}_{4W}^{-\alpha,\boldsymbol{V}}[\boldsymbol{Y}_0] = \omega_0^{-\alpha,\boldsymbol{V}}\boldsymbol{Y}_0 + \omega_1^{-\alpha,\boldsymbol{V}}\boldsymbol{Y}_1 + \omega_2^{-\alpha,\boldsymbol{V}}\boldsymbol{Y}_2 + \omega_3^{-\alpha,\boldsymbol{V}}\boldsymbol{Y}_3 \tag{3}$$

由 $\boldsymbol{X}_0$、$\boldsymbol{X}_1$、$\boldsymbol{X}_2$、$\boldsymbol{X}_3$ 的关系,不难证明 $\boldsymbol{Y}_0$、$\boldsymbol{Y}_1$、$\boldsymbol{Y}_2$、$\boldsymbol{Y}_3$ 分别为 $\boldsymbol{Y}_0$ 的 0 ~ 3 次 DFT。

令 $\boldsymbol{X}_l$ 的复数表达式 $\boldsymbol{X}_l = p_l + \mathrm{i}\cdot q_l$,$(l = 0,1,2,3)$,假设 $\boldsymbol{X}_0$ 在复平面上规则分布,$\boldsymbol{X}_2$ 为 $\boldsymbol{X}_0$ 的反转序列,则其分布也是规则的,而 $\boldsymbol{X}_1$ 与 $\boldsymbol{X}_3$ 遵从高斯分布。p_l 与 q_l 的随机性组合使得 $\boldsymbol{Y}_0$ 在加权系数 $\omega_l^{\alpha,\boldsymbol{V}}$ 的作用下,在复平面呈现出分散(聚拢)、拉伸(压缩)等不同状态。

这里给出一个例子,当采用 QPSK 调制时,p_0、q_0、p_2 以及 q_2 为固定值。首先,考虑式(1)中第 1 项与第 3 项之和,共有 16 种可能值,如图 1(b)所示,这两项之和在复平面上的点可以看作是原始星座点各分裂成 4 个新的星座点。

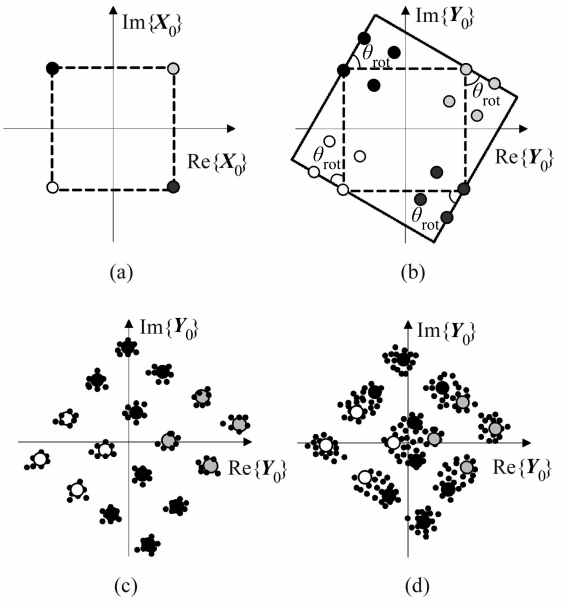

图 1　4-WFRFT 信号复平面示意图

Fig. 1　4-WFRFT signals in complex plane

新的星座图整体沿角度 θ_{rot} 旋转分裂,其旋转角度可以由 $\omega_0^{\alpha,\boldsymbol{V}}$ 计算得到:

$$\theta_{\mathrm{rot}} = \arctan\frac{\mathrm{Im}[\omega_0^{\alpha,\boldsymbol{V}}]}{\mathrm{Re}[\omega_0^{\alpha,\boldsymbol{V}}]} = \frac{\pm 3\pi\alpha\mathrm{i}}{4} \tag{4}$$

然后,考虑式(1)中第 2 项与第 4 项之和,其在复平面上的星座图为类高斯分布,覆盖范围由 α 与 $\boldsymbol{V}$ 共同决定。如图 1(c)与 1(d)所示,$\boldsymbol{Y}_0$ 的星座图随着不同的分裂距离和不同的覆盖范围发生变化,即随着 α 与 $\boldsymbol{V}$ 不断变化。

2　TDCS 安全传输方案

假设 1　非法用户与合法用户所处环境相同,即产生的基函数一致。

假设 2　合法发送端和接收端均采用 4-WFR-

FT,如图2虚线所示,非法接收端仍采用DFT,参数 α 与 $\boldsymbol{V}$ 仅由合法用户预共享。

作为一种频域调制频域编码(spectrally modulated,spectrally encoded,SMSE)信号,TDCS的数据调制和编码可以在IDFT之前的频域实现[11],图2为其系统框图,虚线部分为所提出的新方案。输入二进制比特数据流 $d_n(n=0,1,\cdots,N-1)$,通过映射器和不同的调制方式,信号的星座分布可映射为复信号符号。设原始输入信号为 $x_n = A_n e^{j\theta_{m,n}} x_n = d_n e^{j\theta_n}, 0 \leq n \leq N-1$,调制方式的不同,其数据符号的星座也就不同。

下面给出TDCS的常用调制方式及其参数取值:若使用MPSK调制则 d_n 为常数,$\theta_n = \dfrac{2\pi m}{M}\Big|_{m=0,1,\cdots,M}$;若使用CCSK调制,则 d_n 为常数,对于 $\forall k \in (0,K-1)$,$\theta_{k,n} = \dfrac{-2\pi mk}{M}\Big|_{m=0,1,\cdots,M}$。

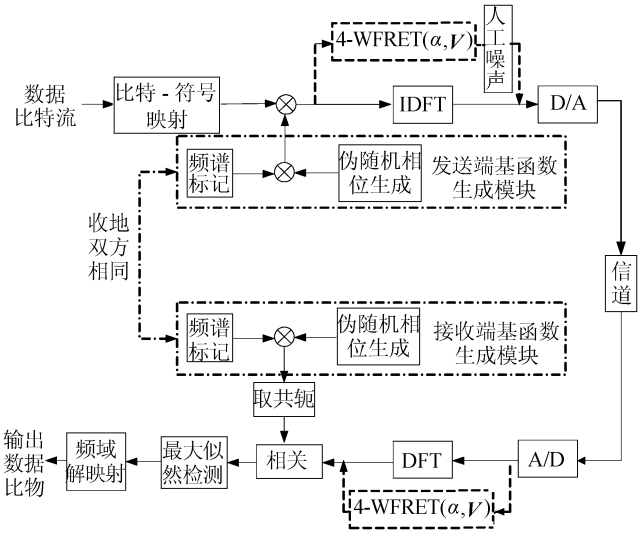

图2 TDCS安全传输方案收发端原理图

Fig.2 Blocks of secure transmission for TDCS

同时,TDCS中的频谱标记 A_k 和伪随机相位 $e^{j\theta_k}$ 均可应利用频谱编码,$\boldsymbol{A} = [A_0, A_1, \cdots, A_{K-1}]$,其生成是对使用频点进行选择,即 $A_k \in (0,1)$,其中,若 $A_k = 0$ 则代表第 k 个频点"不可用",否则 $A_k = 1$。伪随机相位向量 $\boldsymbol{P} = (e^{j\theta_0}, e^{j\theta_1}, \cdots, e^{j\theta_{K-1}})$ 是对每个频点的相位在单位圆上进行旋转,其中,$\theta_k \in \left[0, \dfrac{2\pi}{2^r}, \dfrac{4\pi}{2^r}, \cdots, \dfrac{2\pi(2^r-1)}{2^r}\right]$ 表示从相位映射器的 2^r 个均匀分布在 $[0,2\pi)$ 的相位点中任选一个。二者的,点乘积构成了基函数(basic function,BF)$\boldsymbol{B} = [B_0, B_1, \cdots, B_{K-1}]$,即:

$$\boldsymbol{B} = \boldsymbol{A} \odot \boldsymbol{P} \tag{5}$$

式中,$\odot$ 表示元素与元素之间点乘。输入符号 x_n 被扩展到基函数 $\boldsymbol{B}$ 的每一个频点上产生了SMSE信号,得到的第 n 个SMSE符号可以表示为:

$$S_k(n) = [x_n B_k]_{k=0}^{K-1} = [A_k d_n e^{j(\theta_n+\theta_k)}]_{k=0}^{K-1} = \begin{cases} [d_n e^{j(\theta_n+\theta_k)}]_{k=1}^{K-1}, & A_k = 1; \\ 0, & A_k = 0 \end{cases} \tag{6}$$

对其进行 K 点IDFT变换,得到TDCS信号

$$\boldsymbol{s}_{\text{TDCS}}(n) = F^{-1}[\boldsymbol{S}(n)] \tag{7}$$

式中,F^{-1} 表示IDFT,$\boldsymbol{S}(n) = [S_0(n), S_1(n), \cdots, S_{K-1}(n)]$。

每个符号都被调制到一个长度为 K 的基函数上。使用参数为 α 和 $\boldsymbol{V}$ 的4-WFRFT调制代替IDFT调制,得到新的TDCS信号,称之为4W-TDCS信号。由式(3)得出4W-TDCS符号可以表示为:

$$\boldsymbol{s}_{\text{4W-TDCS}}(n) = F_{\text{4W}}^{\alpha,\boldsymbol{V}}[\boldsymbol{S}(n)] = \omega_0^{\alpha,\boldsymbol{V}}\boldsymbol{S}(n) + \omega_1^{\alpha,\boldsymbol{V}}\boldsymbol{S}_1(n) + \omega_2^{\alpha,\boldsymbol{V}}\boldsymbol{S}_2(n) + \omega_3^{\alpha,\boldsymbol{V}}\boldsymbol{S}_3(n) \tag{8}$$

式中,$F_{\text{4W}}^{\alpha,\boldsymbol{V}}$ 表示参数为 α 和 $\boldsymbol{V}$ 的4-WFRFT,$\boldsymbol{S}_1(n)$、$\boldsymbol{S}_2(n)$、$\boldsymbol{S}_3(n)$ 分别是 $\boldsymbol{S}(n)$ 的1~3次DFT。

随后,加入的人工噪声大小由TDCS频谱感知模块得到的信道状态决定,表示为:

$$\boldsymbol{n}_{\text{artfl}}(n) = \frac{\boldsymbol{H}_n}{P} \tag{9}$$

式中,$\boldsymbol{H}_n = |\boldsymbol{H}_n| e^{j\varphi_{\boldsymbol{H}_n}}$ 为信道估计结果,P 为噪声的相对功率。例如,可以设置噪声功率为 $P = 10^3$ 即比信号功率小30 dB。

最终发送的信号为:

$$\boldsymbol{s}_{\text{trans}}(n) = \boldsymbol{s}_{\text{4W-TDCS}}(n) + \boldsymbol{n}_{\text{art}}(n) \tag{10}$$

相应地,在接收端采用参数 $-\alpha$ 与 $\boldsymbol{V}$ 的4-WFRFT恢复原发送序列为:

$$\boldsymbol{S}(n) = F_{\text{4W}}^{-\alpha,\boldsymbol{V}}[\boldsymbol{s}_{\text{trans}}(n)] \tag{11}$$

经过相关解调后,得到原输入数据。

3 系统性能分析

由于多参数4-WFRFT情况下信号变换较为复杂,下面只对单参数4-WFRFT情况下的TDCS系统性能进行研究。

3.1 误码率分析

若系统采用MPSK调制,TDCS系统误码率为:

$$p_{\text{b}} \approx Q\left(\sqrt{2SNR}\sin\frac{\pi}{M}\right) \tag{12}$$

若采用CCSK调制,则TDCS系统误码率为:

$$p_{\text{b}} \leq (M-1)Q(\sqrt{SNR}) \tag{13}$$

式中,M 为调制阶数,SNR 为接收端信噪比。在式(1)中,对于非目的接收机,第 2 项视为有用信号,其余 3 项可视为噪声。由于傅里叶变换前后能量守恒,$\boldsymbol{S}(n)$ 以及 $\boldsymbol{S}_l(n)(l=1,2,3)$ 的功率相同均为 P_l,又由于 WFRFT 变换后,输入序列在复平面会呈现出旋转分裂的变化,故对非法用户接收造成影响,其影响因子为 $\cos\theta_{\text{rot}}$。根据能量守恒定律,$(|\omega_0^{\alpha,V}|^2+|\omega_1^{\alpha,V}|^2+|\omega_2^{\alpha,V}|^2+|\omega_3^{\alpha,V}|^2)\cos^2\theta_{\text{rot}}=1$。对非目的接收机而言,有用信号经过 4-WFRFT 后的等效能量变为:

$$P_{\text{e}}=|\omega_1^{\alpha,V}|^2\cos^2\theta_{\text{rot}}P_l \tag{14}$$

若采用单参数 4-WFRFT,则有:

$$P_{\text{e}}=|\omega_1^{\alpha,V}|^2\cos^2\theta_{\text{rot}}P_l=\cos^2\frac{\pi(\alpha-1)}{4}\cos^2\frac{\pi(\alpha-1)}{2}\cos^2\frac{3\pi\alpha}{4}P_l \tag{15}$$

非目的接收机的信噪比为:

$$SNR_{\text{e}}=\frac{\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4})P_l}{(1-\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4}))P_l+N_{\text{e}}} \tag{16}$$

由假设 1 可知输入二进制比特数据流长度 $N_l=N_{\text{e}}$,则有非法接收端 CCSK 误码率为:

$$p_{\text{e}}=(M-1)\cdot Q\left(\sqrt{\frac{\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4})}{1-\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4})+\frac{1}{SNR_l}}}\right) \tag{17}$$

MPSK 误码率为:

$$p_{\text{e}}=Q\left(\sin\frac{\pi}{M}\cdot\sqrt{\frac{2\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4})}{1-\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cos^2(\frac{3\pi\alpha}{4})+\frac{1}{SNR_l}}}\right) \tag{18}$$

图 3 为不同信噪比下 BCSK 的 p_{e} 理论值随 α 变化的曲线。

由图 3 可以看出:α 在[0.7,2]区间内 p_{e} 的变化最为剧烈;当 α 为 1.2 时,p_{e} 最小;当 α 为 0、2、3 或 4 时,可使非法接收端得到最大误码率,且随着信噪比的升高,p_{e} 的变化幅度也增大。

3.2　保密容量分析

保密容量表示单位时间内合法用户之间信息可靠传输且保证非法接收者不能正确解调信息的最大速率。由文献[12]中的定义:

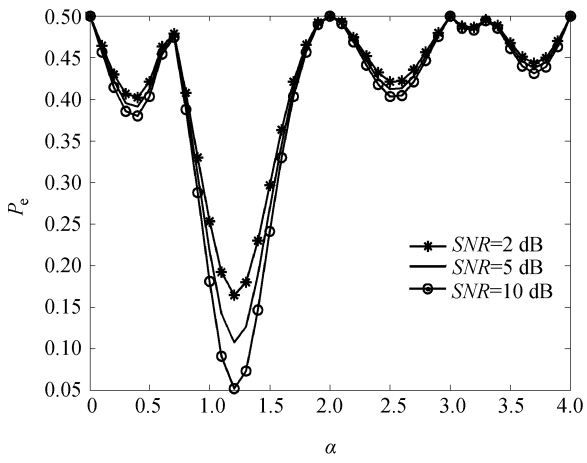

图 3　α 周期内 p_{e} 理论值变化曲线

Fig. 3　Changing curves of theoretical p_{e} in a period of α

$$C_{\text{s}}=C_l-C_{\text{e}} \tag{19}$$

式中,$C_l=\text{lb}(1+P_l/N_l)$ 和 $C_{\text{e}}=\text{lb}(1+P_{\text{e}}/N_{\text{e}})$ 分别为合法用户和非法用户的信道容量,P_l/N_l 与 $P_{\text{e}}/N_{\text{e}}$ 分别为其对应的信噪比。于是有:

$$C_{\text{s}}=\text{lb}(1+P_l/N_l)-\text{lb}(1+P_{\text{e}}/N_{\text{e}}) \tag{20}$$

由式(20),得到保密容量为:

$$C_{\text{s}}=\text{lb}(1+\frac{P_l}{N_l})-\text{lb}(1+\frac{|\omega_1|^2\cos^2\theta_{\text{rot}}P_l}{(1-|\omega_1|^2\cos^2\theta_{\text{rot}})P_l+N_{\text{e}}}) \tag{21}$$

由假设 1 可知 $N_l=N_{\text{e}}$,式(21)可化简为:

$$C_{\text{s}}=\text{lb}[1-\cos^2(\frac{\pi(\alpha-1)}{4})\cos^2(\frac{\pi(\alpha-1)}{2})\cdot\cos^2(\frac{3\pi\alpha}{4})+\frac{1}{SNR_l}] \tag{22}$$

若 C_{s} 为正值,表示系统将信号传送给合法用户的同时可以避免非法用户的窃听;若 C_{s} 为负值,表示非法用户可以窃听到有用信息,系统是不安全的。因此,C_{s} 的值越大,系统越安全。图 4 为不同信噪比下 C_{s} 理论值随 α 变化的曲线。由图 4 可以看出,当 $SNR=2$ dB,α 处于[0,1]或[1.4,4]区间内时 $C_{\text{s}}>0$,表明此时可以保证系统的安全性;同时,随着 SNR 的增大,α 可选取区间变小,这是因为随着 SNR 的提高,窃听者的误码率会减小,因此保密容量相应下降。

4　仿真验证

仿真条件为:

1)发送 100 000 个随机生成的二进制比特数据

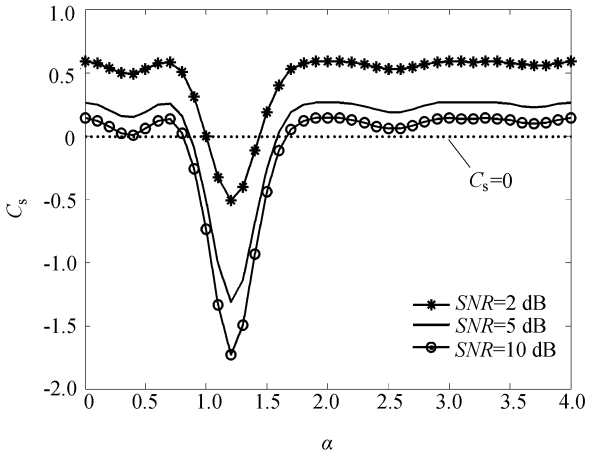

图4 α 周期内 C_s 理论值变化曲线

Fig. 4 Changing curves of theoretical C_s in a period of α

用于仿真误码率性能;

2)基函数在数据发送时间内保持不变,长度为256,频谱幅值成偶对称;

3)合法/非法接收端均已同步。

在无人工噪声且全频谱利用的情况下,采用4-WFRFT的TDCS误码性能随着信噪比变化的对比见图5,仿真中采用BPSK调制。由图5可看出,合法用户误码率远低于非法用户。当α = 1.2,非法用户的误码率是最低的,此结果与第3.1节的理论分析结果一致。当*SNR* = 16 dB,α = 1.2时,非法用户的误码率为0.023,这与无线通信最低限度误码率10^{-4} ~ 10^{-3}相差较远。当α取除1.2以外其他值的情况下,非法用户的误码率都大于0.1且不随*SNR*的增大而发生改变,这说明在非法用户刻意提高信噪比的情况下,本文方法也可以保证TDCS系统的安全性。

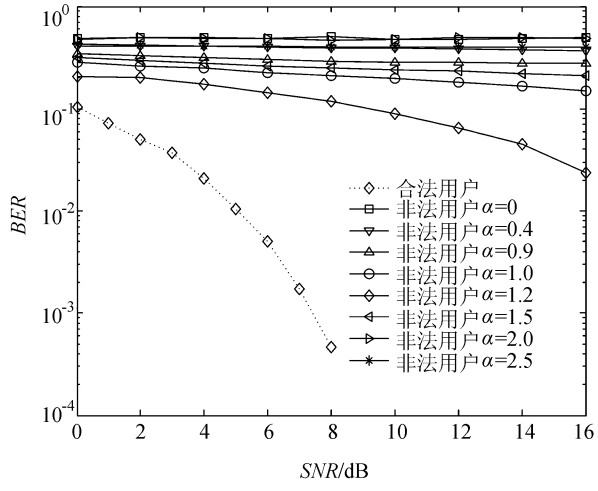

图5 仅采用4-WFRFT的TDCS误码率

Fig. 5 *BER* of TDCS with only 4-WFRFT

在图5中,当采用的4-WFRFT时,一旦*SNR*足够高,非法用户就有可能解调出有用信息,因此,在4-WFRFT后添加人工噪声以进一步增强系统安全性。在全频谱利用和频谱失配情况下,同时采用α = 0.4的4-WFRFT和人工噪声后的TDCS与原TDCS误码性能随着信噪比变化的对比见图6和7。

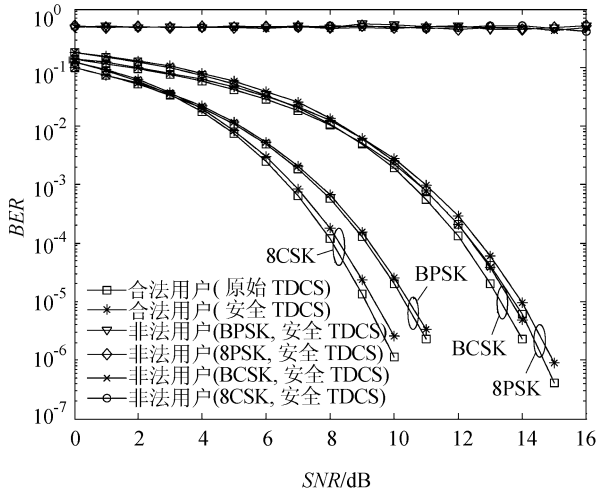

图6 全频谱利用TDCS安全传输方案误码率

Fig. 6 *BER* of secure TDCS without spectrum mismatch

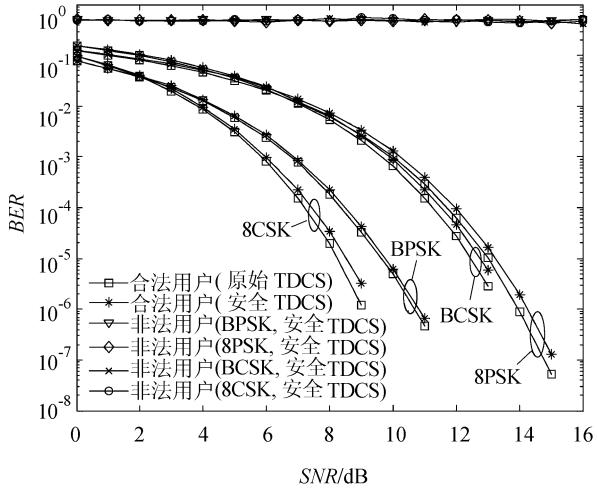

图7 频谱失配TDCS安全传输方案误码率

Fig. 7 *BER* of secure TDCS with spectrum mismatch

如图6~7所示,由于人工噪声的加入,与图5相比,采用BCSK调制时,非法用户误码率由原来的0.39提高到0.5;且无论使用哪种调制方式,本文提出的TDCS安全传输方法中,非法用户的误码率保持在0.5左右,表明非法用户无法解调出有用信息。

与原始TDCS相比,无论使用哪种调制方式,当*BER*为1×10^{-4}时,其信噪比损失小于0.2 dB,可以忽略不计。即使在频谱失配15%的情况下,本文方法与原始TDCS的*BER*性能也近乎相同,说明本文方法同样适用于频谱失配的情况。

分析了不同 α 条件下同时采用人工噪声和 4-WFRFT 的 TDCS 保密容量见图 8。由图 8 可以看出:随着信噪比的增大保密容量都会不同程度地降低,这与第 3.2 节的分析结果一致;在低信噪比下任何 α 取值都可以保证 TDCS 保密容量为正数,但是,在信噪比较高的条件下,要避免选取[0.8,1.7]区间的 α 以保证 TDCS 保密容量为正。

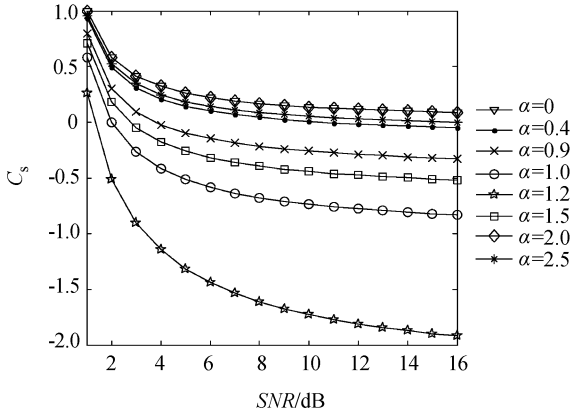

图 8　不同 α 条件下系统保密容量

Fig. 8　Security capacity for secure TDCS with varying α

5　结　论

提出一种 TDCS 的物理层安全传输方法,同时采用 4-WFRFT 和人工噪声以增强系统的安全性。先通过 4-WFRFT 使有用信号复平面分布发生变化,再添加不可逆的人工噪声进一步混淆有用信号的分布,使窃听者无法正确解调有用信号。与原始 TDCS 相比,对于合法用户本文方法保持原系统复杂度的同时产生的信噪比损失可忽略不计,在一定的参数范围内,使保密容量为正数,为需要安全性较高的 TDCS 商业或者军事应用提供了一种可靠方案。在下一步研究中,将考虑多参数变换情况下的 TDCS 的安全性能以及 M 周期的 WFRFT 变换下的 TDCS 的安全性能,以期获得更好的安全传输方法。

参考文献:

[1] Radcliffe R A. Design and simulation of a transform domain communication system[D]. Ohio: Air Force Institute of Technology(AU), 1996.

[2] Richard K M, Marshall H. Reduction of peak-to-average power ratio in transform domain communication systems [J]. IEEE Transactions on Wireless Communications, 2009, 8(9): 4400 – 4405.

[3] Hu Su, Bi Guoan, Guan Yongliang, et al. TDCS-based cognitive radio networks with multiuser interference avoidance [J]. IEEE Transactions on Communications, 2013, 61(12): 4828 – 4835.

[4] Fumat G, Charge P, Zoubir A, et al. Transform domain communication systems from a multidimensional perspective, impacts on bit error rate and spectrum efficiency [J]. IET Commununications, 2011, 5(4): 476 – 483.

[5] Wang Chuandan, Zhang Zhongpei, Li Shaoqian. A new method of basis function generation and its performance analysis[J]. Journal of University of Electronic Science and Technology of China, 2006, 35(4): 648 – 652. [王传丹,张忠培,李少谦. 一种新的基函数产生方法与性能分析[J]. 电子科技大学学报, 2006, 35(4): 648 – 652.]

[6] He Shibiao, Ji Ye, Pan Hui. A method to generate pseudo-random phases in transform domain communication system by chaos mapping[J]. Journal of Chongqing University, 2008, 35(12): 1381 – 1385. [何世彪,季烨,潘辉. TDCS 中随机相位的混沌产生方法[J]. 重庆大学学报, 2008, 35(12): 1381 – 1385.]

[7] Sun Haixin, Bi Guoan, Guan Yongliang, et al. Novel pseudorandom phase generation in transform domain communication systems [C]//Proceedings of 2011 International Conference on Innovations in Information Technology. Abu Dhabi: IEEE, 2011: 18 – 22.

[8] Mei Lin, Sha Xuejun, Ran Qinwen, et al. Research on the application of 4-weighted fractional Fourier transform in communication system[J]. Science China Information Sciences, 2010, 53(6): 1251 – 1260.

[9] Fang Xiaojie, Sha Xuejun, Li Yong. Secret communication using parallel combinatory spreading WFRFT [J]. IEEE Communications Letters, 2015, 19(1): 62 – 65.

[10] Goel S, Negi R. Guaranteeing secrecy using artificial noise[J]. IEEE Transanctions on Wireless Communications, 2008, 7(6): 2180 – 2189.

[11] Chakravarthy V, Nunez A S, Stephens J P. TDCS, OFDM, and MC-CDMA: A brief tutorial[J]. IEEE Radio Communications, 2005, 43(9): 11 – 16.

[12] McLaughlin S W, Rodrigues M R D, Barros J, et al. Wireless information—Theoretic security, information theory[J]. IEEE Transactions on Information Theory, 2008, 54(6): 515 – 534.

(编辑　赵　婧)