

一种 TR-OFDM 系统的四元数加密算法

陈善学, 杜文正, 冯叶青, 李方伟

(重庆邮电大学通信与信息工程学院, 重庆 400065)

摘要: 为了保障时间反演正交频分复用 (Time reversal-orthogonal frequency division multiplex, TR-OFDM) 系统的物理层安全传输, 提出了一种基于四元数加密的安全传输算法。该算法主要分为 3 个步骤: 发射端和合法接收端利用估计信道得到加密传输过程中需要的四元数, 即密钥; 发射端将需要传输的比特序列做三维映射, 利用四元数对三维星座点做旋转加密, 调制为 OFDM 符号并经过时间反演处理之后发射出去; 合法用户利用四元数进行解密和解调, 从而获得传输的数据, 而窃听者因为不知道密钥而无法获得传输信息。因此所提算法保证了系统数据传输的安全性。通过仿真证明本文所提出算法可以使窃听用户的误符号率始终保持在 0.5 左右; 在相同信噪比下, 较传统的二维调制, 合法用户可以实现更低的误符号率; 相较于人工噪声技术方案, 本文所提算法不会影响合法用户的误符号率。

关键词: 时间反演; 正交频分复用; 三维星座旋转; 四元数

中图分类号: TP918 **文献标志码:** A

Quaternion Encryption Algorithm for TR-OFDM System

CHEN Shanxue, DU Wenzheng, FENG Yeqing, LI Fangwei

(College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: In order to ensure the safe transmission of the time reversal-orthogonal frequency division multiplex (TR-OFDM) system, this paper proposes a secure transmission algorithm based on quaternion encryption. The scheme is mainly divided into three steps. In the first step, the transmitter and the legitimate receiver use the estimated channel to obtain the quaternion required in the process of encrypted transmission, that is, the key. In the second step, the transmitting end takes the bit sequence to be transmitted three-dimensional mapping, then uses the quaternion to rotate and encrypt the three-dimensional constellation points, and finally modulates them into OFDM symbols and transmits them after time inversion processing. In the third step, the legitimate user uses the quaternion to decrypt and demodulate to obtain the transmitted data. The eavesdropper cannot obtain the transmission information because they do not know the key. Therefore, the proposed scheme ensures the security of system data transmission. The simulation results show that the proposed algorithm can keep the bit error

rate of eavesdropping users at about 0.5. Under the same SNR, legal users can achieve a lower bit error rate than traditional two-dimensional modulation. Compared with the artificial noise scheme, the proposed algorithm will not affect the bit error rate of legitimate users.

Key words: time inversion; orthogonal frequency division multiplexing; three-dimensional constellation rotation; quaternion

引言

随着无线通信技术的迅猛发展,人们对通信的速率和安全也提出了更高的要求。而根据通信理论,二进制数据传输的速度首先取决于基带的调制方式,通常调制方式越高数据传输速率越快,但其调制的各个参数(振幅、相位和频率)之间的相互影响也越严重,误码率也越高,要保障其传输质量只能通过提高信噪比或采用更加复杂的接收技术。而高维信号在信号能量相等的情况下,可以实现更低的误码率并且可以在实际环境中实现更加高效和可靠的通信^[1-2]。同时物理层中由于信道固有的开放性与广播性,使得物理层成了通信系统中最脆弱的一环,因此物理层安全也引起了学术界的广泛研究。物理层安全中的星座旋转是一种调整信号星座使窃听者无法正确解码接收到的信息的技术^[3],目前对于调制信号的加密方式主要有相位旋转^[4]、幅相变换^[5]和星座间跳转^[6]。而文献[5-6]复杂度较高,实现起来比较困难。文献[7]对调制信号进行星座旋转并添加少许人工噪声以保证 OFDM 系统的安全,但人工噪声会降低信道资源的利用率,文献[8-9]研究了 QPSK 信号的三维星座设计并推导了三维星座点的误码率。文献[10-11]设计了高阶的三维信号星座,相比于传统的二维星座,三维星座可以在相同信号能量前降低误码率。而传统的调制方式,随着调制阶数的增大,星座信号之间的最小欧式距离(Minimum euclidean distance, MED)逐渐减少,致使信号在信道中的鲁棒性受到了损害,信号的误码率开始逐渐增大,而三维星座可以在相同误码率的前提下实现更高的吞吐量,并且提高了信号的鲁棒性。这使得三维信号星座在提高信息传输速率方面具有重大的潜力,尤其是对于数据较大的文件(如音频、视频和压缩包等)的传输具有重大意义。而文献[12]将三维星座分别绕 x 轴、 y 轴和 z 轴旋转不同的角度,这种算法每个星座点需要依次乘以 3 个三维旋转矩阵,空间复杂度太高。而四元数可以实现绕任意轴的旋转^[13-14],且其所需的内存远小于 3 个三维旋转矩阵。而时间反演(Time reversal, TR)等效于一个空时匹配滤波器,可以降低 OFDM 系统的误码率,减小循环前缀长度。故本文针对 TR-OFDM 系统,提出了一种四元数加密的物理层加密传输算法。

1 系统模型

本文的 TR-OFDM 系统模型主要有 3 个节点,如图 1 所示:基站是 Alice,合法用户 Bob,而 Bob 附近有一个潜在的窃听者 Eve, Eve 的位置和信道状态信息未知。Bob 和 Eve 都只配备一根天线,基站 Alice 与合法用户 Bob 需要实现安全传输通信。设 Alice 到 Bob 之间的信道为主信道, Alice 与 Eve 之间的信道为窃听信道。假设 Alice 和 Bob 采用时分双工(Time division duplex, TDD)通信模式,通信双方 Alice 和 Bob 利用估计到的信道状态信息生成加密和解密所需的四元数。根据本文所采用的安全传输模型,采用 N 个子载波传输的传输 OFDM 符号。主信道和窃听信道都是瑞利多径信道。

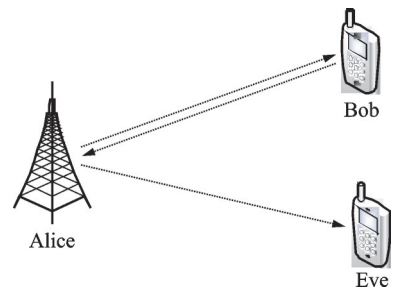


图 1 系统模型

Fig.1 System model

2 四元数加密算法

三维 TR-OFDM 系统如图 2 所示。

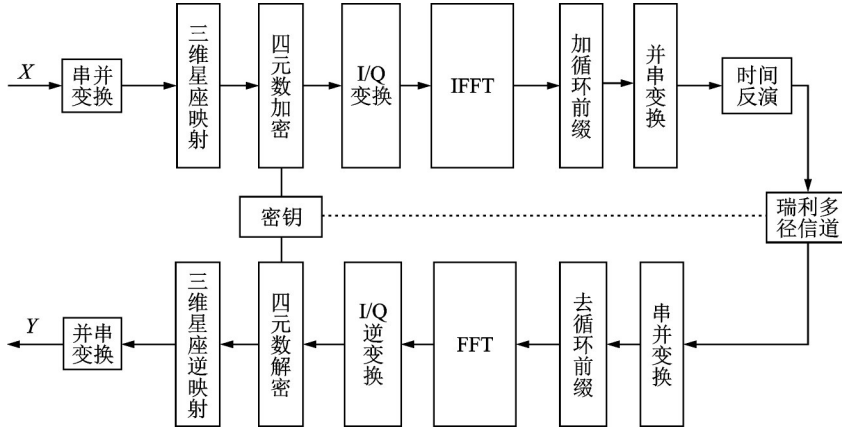


图 2 三维 TR-OFDM 系统方框图

Fig.2 Block diagram of three-dimensional TR-OFDM system

假设 Alice 需要传输一组比特序列, 先将二进制序列进行串并变换, 然后把每 M 个比特映射为一个三维的信号 $s_i = [x_i \ y_i \ z_i]^T$ 。将每个三维星座点进行四元数加密后的星座点 $s'_i = [x'_i \ y'_i \ z'_i]^T$ 表示为

$$s'_i = q s_i q^{-1} \tag{1}$$

式中: q 为四元数, $q = [q_0 \ q_1 \ q_2 \ q_3]$, s'_i 等效于三维星座点 s_i 绕轴 n 旋转 θ 后的三维星座点。

$$n = \begin{bmatrix} \frac{q_1}{\sqrt{1-q_0^2}} & \frac{q_2}{\sqrt{1-q_0^2}} & \frac{q_3}{\sqrt{1-q_0^2}} \end{bmatrix} \tag{2}$$

$$\theta = \arccos(q_0) \tag{3}$$

式中: q^{-1} 为四元数的逆, $q^{-1} = q^* / \|q\|$; q^* 为四元数的共轭, $q^* = [q_0 \ -q_1 \ -q_2 \ -q_3]$; $\|q\|$ 为四元数的模长, $\|q\| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$ 。

图 3 是加密前 4-ary 的三维星座点, 4 个三维星座点均匀分布在一个半径为 1 的球面上, 并且 4 个点刚好构成一个正四面体。图 4 是加密后 4-ary 的三维星座点, 三维星座点经过四元数加密, 随机地分布在半径为 1 的球面上。图 5 是加密前 16-ary 的三维星座点分布, 16 个点分别在两个不同半径的球面上, 每个球面上 8 个点, 而且每个球面上的 8 个点刚好构成一个正方体。图 6 是加密后 16-ary 的三维星座点分布, 16-ary 的三维星座点经过旋转加密后, 随机地分布在两个球的球面上。接着对加密过的信号 $s'_i = [x'_i \ y'_i \ z'_i]^T$ 进行 I/Q 变换 (I: 同相分量, Q: 正交分量)。加密过的信号 s' 为

$$s' = [s'_1 \ s'_2 \ \dots \ s'_N] \tag{4}$$

I/Q 转换后的信号 s'' 为

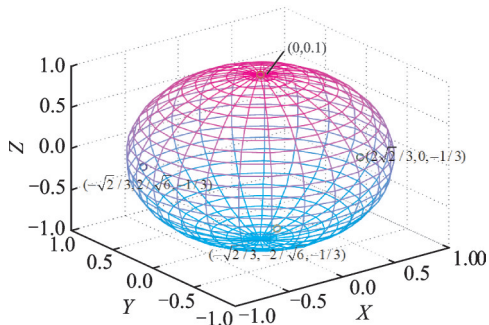


图3 加密前的三维信号(4-ary)

Fig.3 Three-dimensional signal before encryption (4-ary)

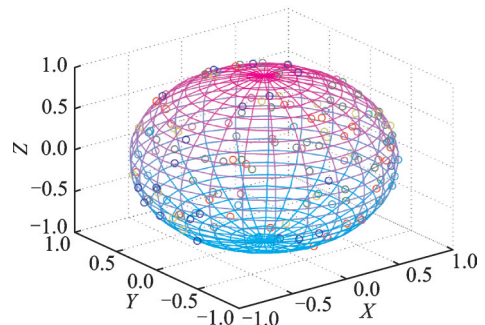


图4 加密后的三维信号(4-ary)

Fig.4 Three-dimensional signal after encryption (4-ary)

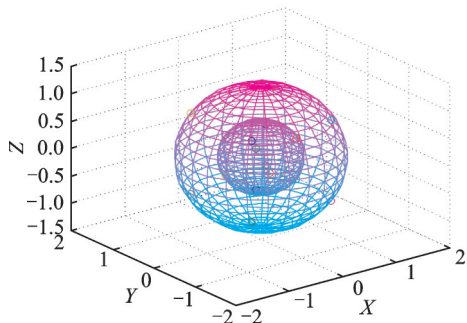


图5 加密前的三维信号(16-ary)

Fig.5 Three-dimensional signal before encryption (16-ary)

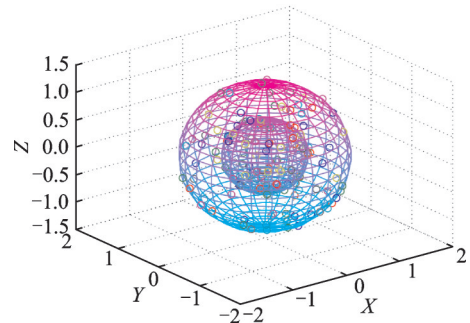


图6 加密后的三维信号(16-ary)

Fig.6 Three-dimensional signal after encryption (16-ary)

$$s'' = \begin{bmatrix} x'_1 + iy'_1 \\ z'_1 + ix'_2 \\ y'_2 + iz'_2 \\ \vdots \\ z'_2 + ix'_{N-1}' \\ y'_N + iz'_N \end{bmatrix} \quad (5)$$

将信号 s'' 进行快速傅里叶逆变换 (Inverse fast fourier transform, IFFT), 为了消除载波间的干扰和符号间干扰加入循环前缀, 在并串变换后通过时间反演操作后发送出去。

Bob 第 k 个子载波上接收到的频域信号为

$$y(k) = s''_k h_r(k)^H h_r(k) + n_r(k) = \frac{|s''_k h_r(k)|^2}{\|h_r(k)\|} + n_r(k) \quad (6)$$

式中: $h_r(k)$ 为 Alice 和 Bob 之间的信道的第 k 个子载波的频域冲激响应; $h_r(k)^H$ 为时间反演镜, 它是主信道在频域的共轭; $n_r(k)$ 是均值为 0、方差为 σ^2 的加性高斯白噪声。

$$\mathbf{h}_r(k)^H = \frac{\mathbf{h}_r(k)^*}{\|\mathbf{h}_r(k)\|} \tag{7}$$

式中: $|\cdot|^*$ 代表共轭, $\|\cdot\|$ 代表 Frobenius 范数。

$$\mathbf{h}_r(k) = \sum_{l=1}^L \alpha_{r,l} e^{-j2\pi k \Delta f \tau_{r,l}} \tag{8}$$

式中: L 为多径总数, α_l 为第 l 条多径的幅度值, Δf 为子载波间隔, τ_l 为第 l 条多径的时延。

Bob 接收到信号后对接收到的信号进行一系列处理(串并变换, 傅里叶变换(Fast fourier transform, FFT), 去循环前缀)后进行阈值判决, 即可得到聚焦的有用信号 s_r'' 。

$$s_r'' = \begin{bmatrix} x_1'' + iy_1'' \\ z_1'' + ix_2'' \\ \vdots \\ z_{N-1}'' + ix_N'' \\ y_N'' + z_N'' \end{bmatrix} \tag{9}$$

接着将信号 s'' 进行 I/Q 逆变换, 重新映射为 N 行 3 列的三维星座点

$$s'_i = [s_1'' \quad s_2'' \quad \cdots \quad s_N''] \tag{10}$$

与发送端相对应, Bob 利用四元数对接收到的信号进行解密, 也就是对三维星座点绕与 n 对称的轴旋转 θ , 进行旋转解密后的信号为 s_i 。

$$s_i = q^{-1} s'_i q \tag{11}$$

解密后的三维星座点, 利用最小距离检测器, 对接收到的信号进行解调得到初始的比特信息。

Eve 第 k 个子载波上接收到的频域信号为

$$\mathbf{y}(k) = s_k'' \mathbf{h}_r^H(k) \mathbf{h}_e(k) + \mathbf{n}_e(k) = \frac{s_k'' \sum_{l=1}^L \alpha_{r,l} \alpha_{e,l} e^{j2\pi k \Delta f (\tau_{r,l} - \tau_{e,l})}}{\|\mathbf{h}_r(k)\|} + \mathbf{n}_e(k) \tag{12}$$

式中: $\mathbf{h}_e(k)$ 为 Alice 和 Eve 之间的信道的第 k 个子载波的频域冲激响应, $\mathbf{n}_e(k)$ 是均值为 0 方差、为 σ^2 的加性高斯白噪声。

$$\mathbf{h}_e(k) = \sum_{l=1}^L \alpha_{e,l} e^{-j2\pi k \Delta f \tau_{e,l}} \tag{13}$$

本文所提出的四元数加密算法流程如图 7 所示。

3 实验仿真

3.1 MED 对比

最小欧氏距离是衡量星座好坏的一个重要标准, 在信号能量相等的条件下, 二维星座图和三维星座图的 MED 参数如表 1 所示。

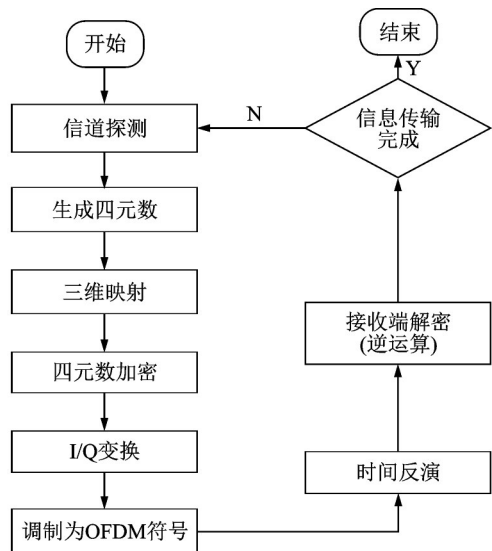


图 7 四元数加密算法

Fig.7 Quaternion encryption algorithm

表1中三维信号星座和二维信号星座的对应关系为: 4-ary \Leftrightarrow QPSK, 16-ary \Leftrightarrow 16QAM, 64-ary \Leftrightarrow 64QAM, 128-ary \Leftrightarrow 128QAM。从表1的MED可以看出在信号能量相等的条件下三维星座图的MED基本上优于二维星座图的MED,尤其对于高阶调制信号,增加比尤其明显。

3.2 实验仿真

本节对三维星座点的四元数加密的算法利用MATLAB进行了仿真,设一帧为6个OFDM符号,每个OFDM符号有128个子载波,循环前缀为32,信道为均值为0,方差为1的瑞利多径信道,信道的多径长度为9,蒙特卡洛次数为10000。

3.2.1 误符号率对比

从图8可见,三维星座信号的误符号率性能相较于二维星座信号都有较大的提升,对于4-ary的信号三维相较于二维在误符号率为 10^{-6} 时提升了约2.5个信噪比,而对于16-ary三维星座信号也提升了约2个信噪比。三维星座信号改善误符号率性能基本上与表1中MED的增加比相符。

3.2.2 误符号率降低比

为了对比二维星座点和三维星座点在相同信噪比下的误符号率性能,本文定义了一个误符号率降低比 η

$$\eta = \frac{e_{3D} - e_{2D}}{e_{2D}} \quad (14)$$

式中: e_{3D} 为三维星座点对应的误符号率, e_{2D} 为二维星座点对应的误符号率。

从图9可知,随着信噪比的增大,误符号率降低比也逐渐增大。4-ary的三维星座点对比于QPSK,当信噪比为12 dB时,误符号率降低比到达下界,而16-ary的三维星座点对比于16QAM,当信噪比为20 dB时,误符号率降低比到达下界。并且4-ary误符号率降低比明显比16-ary的误符号率降低比下降的快。与表1中4-ary和16-ary的MED增加比相对应。

3.2.3 误符号率

本文所采用的四元数加密算法和文献[15]的人工噪声(Artificial noise, AN)方案误符号率对比如图10所示,随着人工噪声的能量比例增大,窃听者的误符号率明显增大,但同时合法用户的误符号率也会受到损害。且当人工噪声的能量比例为90%时,尽管窃听者的误符号率也保持在较高的水平,但仍低于本文所提的方案。而合法用户的误符号率却受到了较大的影响。

3.2.4 保密传输速率

根据文献[16]对于二进制广播信道的保密传输速率为

表1 最小欧式距离

星座图	2D	3D	增加比/%
4-ary	1.414 2	1.633 0	15.5
16-ary	0.632 5	0.687 4	8.7
64-ary	0.308 6	0.516 4	67.3
128-ary	0.220 9	0.408 3	84.8

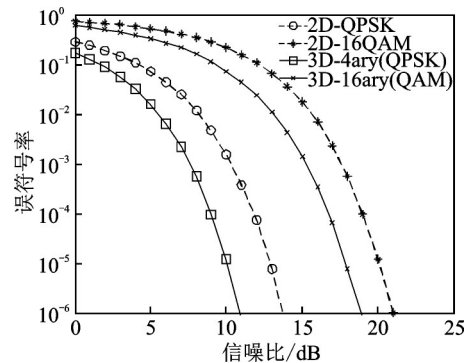


图8 三维星座信号与传统二维星座信号误符号率对比图

Fig.8 Comparison of symbol error rate between 3D constellation signal and traditional 2D constellation signal

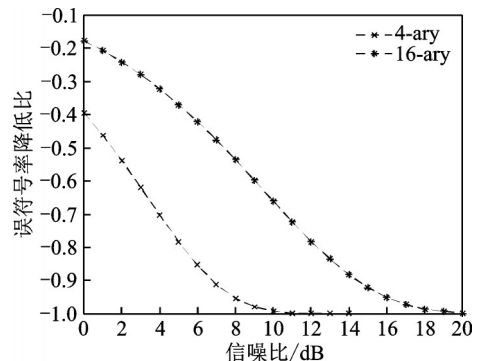


图9 误符号率降低比

Fig.9 Symbol error rate reduction ratio

$$C_s = H(e_{AE}) - H(e_{AB}) = -e_{AE} \log_2(e_{AE}) - (1 - e_{AE}) \log_2(1 - e_{AE}) + e_{AB} \log_2(e_{AB}) + (1 - e_{AB}) \log_2(1 - e_{AB}) \quad (15)$$

式中: e_{AB} 为合法用户 Bob 的误符号率, e_{AE} 为窃听用户 Eve 的误符号率。本文对 4-ary 的三维星座点和 16-ary 的三维星座点所对应的保密传输速率进行了仿真。仿真结果如图 11 所示。

从图 11 可知, 文献[15]的人工噪声方案的人工噪声能量比例较小时, 其归一化保密传输速率随着信噪比增大, 逐渐减小, 但是当人工噪声的比例为 90% 时, 人工噪声方案的归一化保密传输速率也开始上升, 但由于人工噪声能量比例过高, 对合法用户的误符号率也有一定的损害, 故其归一化保密传输速率依旧低于本文所提算法。

4 结束语

为了保障 TR-OFDM 系统的物理层安全传输, 本文提出一种四元数加密算法, 首先对 TR-OFDM 的系统模型进行了描述, 其次在该模型下, 对本文的四元数加密算法步骤进行了详细的说明, 最后对四元数加密算法的误符号率和保密传输速率进行了仿真, 并与传统的二维星座误符号率进行了对比。通过仿真表明: 随着信噪比的增大, 本方案可以使窃听者难以获得合法通信双方通信的任何信息, 且具有一定的保密传输速率, 而合法用户可以获得比传统的二维星座信号更优的误符号率。相较于人工噪声方案, 本文所提算法不会影响合法用户的误符号率, 这对于提高数据传输速率具有重要的意义, 在下一代通信或者军事安全通信中具有重大的潜力。

参考文献:

- [1] GUO Shuaishuai, ZHANG Haixia, ZHANG Peng, et al. Generalized 3-D constellation design for spatial modulation[J]. IEEE Transactions on Communications, 2017, 65(8): 3316-3327.
- [2] 张祥莉, 王勇, 王典洪, 等. 四维信号星座图改进及相应 OFDM 系统模型设计[J]. 电子学报, 2020, 48(8): 1486-1492. ZHANG Xiangli, WANG Yong, WANG Dianhong, et al. Improvement of four-dimensional signal constellation diagram and corresponding OFDM system model design[J]. Chinese Journal of Electronics, 2020, 48(8): 1486-1492.
- [3] 奚晨婧, 高媛媛, 沙楠, 等. 物理层安全信号星座的设计方法研究[J]. 小型微型计算机系统, 2018, 39(12): 2675-2680. XI Chenjing, GAO Yuanyuan, SHA Nan, et al. Research on the design method of physical layer security signal constellation [J]. Small Microcomputer System, 2018, 39(12): 2675-2680.
- [4] HUO Fei, GONG Gong. XOR encryption versus phase encryption, an in-depth analysis[J]. IEEE Transactions on Electromagnetic Compatibility, 2015, 57(4): 903-911.
- [5] 雷蓓蓓. 基于物理层加密的调制方式隐藏算法研究[D]. 西安: 西北大学, 2012.

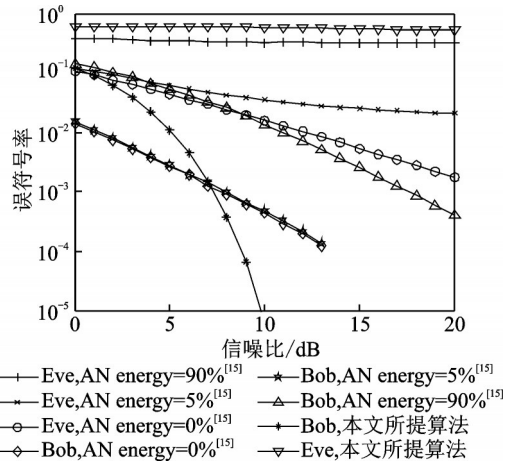


图 10 人工噪声方案和本文算法的误符号率性能对比

Fig.10 Comparison of symbol error rate performance of the artificial noise scheme and the proposed algorithm

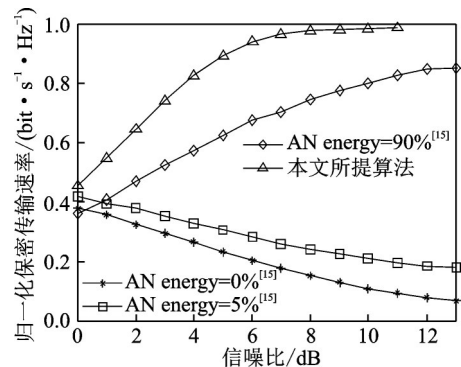


图 11 保密传输速率和人工噪声方案归一化保密传输速率对比

Fig.11 Comparison of secret transmission rate and the normalized secret transmission rate of the artificial noise scheme

- LEI Beibei. Research on modulation concealment algorithm based on physical layer encryption[D]. Xi'an: Northwest University, 2012.
- [6] 岳敖, 李为, 马东堂, 等. 拉丁阵和幅相变换相结合的物理层加密传输算法[J]. 信号处理, 2016, 32(6): 660-668.
YUE Ao, LI Wei, MA Dongtang, et al. Physical layer encryption transmission algorithm combining Latin matrix and amplitude-phase transformation[J]. Signal Processing, 2016, 32(6): 660-668.
- [7] MA Ruifeng, DAI Linglong, WANG Zhaocheng, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion[J]. IEEE Transactions on Consumer Electronics, 2010, 56(3): 1328-1332.
- [8] CHEN Zhenxing, CHOI E C, KANG S G. Closed-form expressions for the symbol error probability of 3-D OFDM[J]. IEEE Communications Letters, 2010, 14(2): 112-114.
- [9] CHEN Zhenxing, KANG S G. Probability of symbol error of OFDM system with 3-dimensional signal constellations[C]//2009 IEEE 13th International Symposium on Consumer Electronics. Kyoto: IEEE, 2009: 442-446.
- [10] KANG S G, CHEN Zhenxing, KIM J Y, et al. Construction of higher-level 3-D signal constellations and their accurate symbol error probabilities in AWGN[J]. IEEE Transactions on Signal Processing, 2011, 59(12): 6267-6272.
- [11] CHEN Bo, JIANG Ming. Design of three-dimensional constellations for wireless communication systems[C]//Proceedings of 2015 IEEE International Conference on Communications. London: IEEE, 2015: 2876-2881.
- [12] 李小倩, 李为, 雷菁, 等. OFDM系统中基于三维星座旋转的物理层安全加密算法[J]. 电子学报, 2017, 45(12): 2873-2880.
LI Xiaoqian, LI Wei, LEI Jing, et al. Physical layer security encryption algorithm based on three-dimensional constellation rotation in OFDM system[J]. Chinese Journal of Electronics, 2017, 45(12): 2873-2880.
- [13] 李志伟, 李克昭, 赵磊杰, 等. 基于单位四元数的任意旋转角度的三维坐标转换[J]. 大地测量与地球动力学, 2017, 37(1): 81-85.
LI Zhiwei, LI Kezhao, ZHAO Leijie, et al. Three-dimensional coordinate conversion based on unit quaternion at any rotation angle[J]. Geodesy and Geodynamics, 2017, 37(1): 81-85.
- [14] 郑军. 四元数和旋转矩阵相互转化的算法实现[J]. 阴山学刊(自然科学), 2012, 26(3): 11-14.
ZHENG Jun. The realization of the algorithm for the mutual conversion of quaternion and rotation matrix[J]. Yinshan Academic Journal (Natural Science), 2012, 26(3): 11-14.
- [15] GOLSTEIN S, NGUYEN T, HORLIN F, et al. Physical layer security in frequency-domain time-reversal SISO OFDM communication[C]//Proceedings of 2020 International Conference on Computing, Networking and Communications. Big Island: IEEE, 2020: 222-227.
- [16] 钟州, 金梁, 黄开枝. 多载波系统随机子载波加权的物理层加密算法[J]. 通信学报, 2012, 33(10): 86-90.
ZHONG Zhou, JIN Liang, HUANG Kaizhi. Physical layer encryption algorithm based on random sub-carrier weighting in multi-carrier systems[J]. Journal on Communications, 2012, 33(10): 86-90.

作者简介:



陈善学(1966-), 男, 博士、教授, 硕士生导师, 研究方向: 数字图像处理, E-mail: chensx@cqupt.edu.cn。



杜文正(1997-), 男, 硕士研究生, 研究方向: 高光谱, E-mail: 1243036841@qq.com。



冯叶青(1995-), 通信作者, 男, 硕士研究生, 研究方向: 物理层安全, E-mail: 1576707825@qq.com。



李方伟(1960-), 男, 教授, 博士生导师, 研究方向: 移动通信安全传输技术, E-mail: lifw@cqupt.edu.cn。