基于CR-WFRFT的物理层安全认证方法

吴佳隆，任清华，李 明
（空军工程大学信息与导航学院，西安，710077）

摘要 作为安全认证的重点研究方向，物理层认证能够节省上层的认证资源，对提高有限资源的利用具有重要意义。针对物理层认证过程安全性不高的问题，提出了一种加权分数傅里叶变换（WFRFT）与星座图旋转角度相结合的物理层认证方法。利用WFRFT的低截获性，基于星座图旋转角度的加权分数傅里叶变换物理层认证系统，能够在不对信号传输过程造成影响的前提下，通过提高计算复杂度降低认证信号的被识别概率。仿真结果表明：经过CR-WFRFT系统输出的信号被识别概率可无限接近于0，且误码率能够与原QPSK理论值相近。CR-WFRFT系统的物理层认证安全性得到了极大提高，进一步保证了信息的有效传输。

关键词 CR-WFRFT；物理层认证；调制水印；信号星座图
DOI 10.3969/j.issn.1009-3516.2020.03.015
中图分类号 TN918.91 **文献标志码** A **文章编号** 1009-3516(2020)03-0093-06

Research on Physical Layer Security Authentication Method Based on CR-WFRFT

WU Jialong, REN Qinghua, LI Ming
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract As the key of security authentication, physical layer authentication can save the authentication resources of the upper layer to play an important role in improving the utilization of limited resources. In view of solving the problem of low security in the process of physical layer authentication, a physical layer authentication method based on weighted-type fractional Fourier transform and rotation angle of constellation is proposed. With the low interception of WFRFT, weighted fractional Fourier transform physical layer authentication system based on rotation angle of constellation can reduce the recognition probability of authentication signal by increasing the computational complexity without affecting the signal transmission process. The simulation results show that the recognition probability of the signal outputted through the CR-WFRFT system can be infinitely close to 0, and the BER can be close to the theoretical value of the original QPSK. The physical layer authentication security of CR-WFRFT system is greatly improved, and further the effective transmission of information is ensured.

Key words CR-WFRFT; physical layer authentication; modulation watermarking; signal constellation

收稿日期：2019-04-26
基金项目：国家重点实验室合作基金(KX162600022)
作者简介：吴佳隆(1996－)，男，辽宁沈阳人，硕士生，主要从事物理层安全研究。E-mail:813544351@qq.com

引用格式：*吴佳隆，任清华，李明. 基于CR-WFRFT的物理层安全认证方法[J]. 空军工程大学学报(自然科学版)，2020，21(3)：93-98. WU Jialong, REN Qinghua, LI Ming. Research on Physical Layer Security Authentication Method Based on CR-WFRFT[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(3): 93-98.*

认证技术作为信息安全的重要保证,一般分为消息认证和身份认证两种。消息认证主要完成数据起源验证并确保接收信息在传输过程中未发生被篡改、重放或延迟等情况。身份认证用于对接入用户的身份鉴别,确保该用户对当前信息的访问使用权限。

随着物理层研究的不断深入,无线信道互易性、唯一性和多样性的特点也为物理层安全技术提供了新的研究思路。物理层认证作为应用层认证机制的有效补充,已经得到了国内外各研究机构的普遍重视。2005 年,日本东北大学的 Kohno[1] 团队以及瑞士苏黎世联邦理工学院的 Capkun 团队[2-3] 利用设备硬件的不完美性提取设备独有的特征,都提出了基于"射频指纹"的认证方案。2008 年,马里兰大学 Baras 团队[4] 为节约频带资源,提高资源利用率,提出了一种基于物理层的数字水印技术,将应用层的认证信息隐藏到信号的幅度或相位信息中。2009 年,电子科技大学的文红团队[5-9] 为弥补物理层和应用层的各自不足,提出并分析了跨层认证的方法。2010 年,美国新泽西州立大学 Trappe 带领的团队[10] 根据信道特征与位置相关短时不变性,提出了一种基于信道指纹的认证方案。2013 年,密歇根大学 Shan 等人[11] 为实现身份认证的安全增强,提出名为"PHY-CRAM"(物理层信道挑战-响应)的认证机制。

本文提出一种基于加权分类傅里叶变换(Weighted Fractional Fourier Transform, WFRFT)的物理层认证方法。在不影响正常信息通信的前提下,将信号星座图旋转角度视为信号"水印"。传输信号经过 WFRFT,可以较为灵活地改变信号原有的统计特征,信号星座图经过旋转、混叠以及高斯化分布之后,对变换后信号检测、调制方式的识别难度将得到很大程度的提高,所得到的信号"水印"也将更加复杂。"水印"复杂度的提高能够在认证过程中起到关键性作用,认证安全性随之提升。

从信号传输的角度来看,这种方法在不影响消息传输效率的重要前提下,仅利用物理层便完成了安全认证,节省了应用层的认证资源,在提高资源利用率的同时,也进一步实现了消息认证和身份认证的安全性提升。

1 CR-WFRFT 基本原理

1.1 星座旋转

星座图作为帮助定义信号元素振幅和相位的有力工具,能够通过同相成分和正交成分的峰值振幅来表征信号元素的特性。在信号处理过程中,当外部输入信号的频率与本地时钟频率不等时,反映在星座图上为星座图出现旋转角度。

假设映射之后存在 S 个星座点,将其中星座图的每一个点表示为 x_i,$i=0,1,\cdots,S-1$,若外部输入信号频率小于本地时钟频率,则进行逆时针旋转,可将旋转角度 θ 之后的星座点表示为 y_i,$i=0,1,\cdots,S-1$,星座点旋转前后的关系可表示为:

$$y_i=x_i\exp(\mathrm{j}\theta),i=0,1,\cdots,S-1 \tag{1}$$

1.2 WFRFT

在 Namias、Mcbride、Kerr 求解 Schrödinger 得到经典分类阶傅时叶变换(Classic Fractional Fourier Transform, CFRFT)之后,Shih 在分数傅里叶变换的基础上提出了经典加权分数傅里叶变换。其定义可以表示为:

$$\mathcal{F}_{4w}^{\alpha}=w_0(\alpha)g(x)+w_1(\alpha)G(x)+w_2(\alpha)g(-x)+w_3(\alpha)G(-x) \tag{2}$$

式中:$g(x)$ 为连续函数;$\mathcal{F}$ 为傅里叶变换;$g(x)$、$G(x)$、$g(-x)$、$G(-x)$ 为加权项,它们之间的相互关系为:

$$\begin{cases}\mathcal{F}^1[g(x)]=G(x)\\ \mathcal{F}^2[g(x)]=\mathcal{F}^1[G(x)]=g(-x)\\ \mathcal{F}^3[g(x)]=\mathcal{F}^1[g(-x)]=G(-x)\\ \mathcal{F}^4[g(x)]=\mathcal{F}^1[G(-x)]=g(x)\end{cases} \tag{3}$$

加权系数 w_l 可定义为:

$$w_l(\alpha)=\cos\left[\frac{(\alpha-1)\pi}{4}\right]\cos\left[\frac{2(\alpha-1)\pi}{4}\right]\cdot\exp\left[\frac{3(\alpha-1)\pi i}{4}\right],(l=0,1,2,3) \tag{4}$$

为了使 WFRFT 适用于数字通信系统,通过对离散傅里叶变换(Discrete Fourier Transform, DFT)算子的分数化直接给出了离散序列的 WFRFT,定义如下:

$$\mathcal{F}_{4W}^{\alpha,V}[\boldsymbol{X}_0]=w_0\boldsymbol{X}_0+w_1\boldsymbol{X}_1+w_2\boldsymbol{X}_2+w_3\boldsymbol{X}_3 \tag{5}$$

式中:$\{\boldsymbol{X}_0,\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_3\}$ 分别是 $\boldsymbol{X}_0$ 的 0~3 次 DFT,则 $\boldsymbol{X}_0$ 是 $\boldsymbol{X}_3$ 的 DFT。DFT 采用能量归一化的定义形式,可将上式重写为:

$$\begin{bmatrix}\boldsymbol{S}_0\\ \boldsymbol{S}_1\\ \boldsymbol{S}_2\\ \boldsymbol{S}_3\end{bmatrix}=\begin{bmatrix}w_0 & w_1 & w_2 & w_3\\ w_3 & w_0 & w_1 & w_2\\ w_2 & w_3 & w_0 & w_1\\ w_1 & w_2 & w_3 & w_0\end{bmatrix}\begin{bmatrix}\boldsymbol{X}_0\\ \boldsymbol{X}_1\\ \boldsymbol{X}_2\\ \boldsymbol{X}_3\end{bmatrix}=\begin{bmatrix}w_0\boldsymbol{X}_0+w_1\boldsymbol{X}_1+w_2\boldsymbol{X}_2+w_3\boldsymbol{X}_3\\ w_3\boldsymbol{X}_0+w_0\boldsymbol{X}_1+w_1\boldsymbol{X}_2+w_2\boldsymbol{X}_3\\ w_2\boldsymbol{X}_0+w_3\boldsymbol{X}_1+w_0\boldsymbol{X}_2+w_1\boldsymbol{X}_3\\ w_1\boldsymbol{X}_0+w_2\boldsymbol{X}_1+w_3\boldsymbol{X}_2+w_0\boldsymbol{X}_3\end{bmatrix} \tag{6}$$

对于任意 N 长复数序列 $\boldsymbol{X}_0=\{x_0,x_1,\cdots,$

$x_{N-1}\}^{\mathrm{T}}$，利用 DFT 矩阵 $\boldsymbol{F}$ 以及反转矩阵定义，可将离散序列 WFRFT 定义式写为：

$$\boldsymbol{S}_0=\mathcal{F}_{4W}^{\alpha,\boldsymbol{V}}[\boldsymbol{X}_0]=$$
$$w_0\ \boldsymbol{F}^0\ \boldsymbol{X}_0+w_1\ \boldsymbol{F}^1\ \boldsymbol{X}_0+w_2\ \boldsymbol{F}^2\ \boldsymbol{X}_0+w_3\ \boldsymbol{F}^3\ \boldsymbol{X}_0=$$
$$w_0\boldsymbol{I}\boldsymbol{X}_0+w_1\boldsymbol{F}\boldsymbol{X}_0+w_2\boldsymbol{I}\boldsymbol{I}\boldsymbol{X}_0+w_3\ \boldsymbol{F}^{\mathrm{H}}\ \boldsymbol{X}_0=$$
$$(w_0\boldsymbol{I}+w_1\boldsymbol{F}+w_2\boldsymbol{I}\boldsymbol{I}+w_3\ \boldsymbol{F}^{\mathrm{H}})\boldsymbol{X}_0=$$
$$\boldsymbol{F}_{4W}(\alpha,\boldsymbol{V})\boldsymbol{X}_0 \tag{7}$$

式中：$\boldsymbol{F}=\frac{1}{\sqrt{N}}\begin{bmatrix}1 & \cdots & 1\\ \vdots & & \vdots\\ 1 & \cdots & Q^{(N-1)(N-1)}\end{bmatrix}$；$Q=\mathrm{e}^{\frac{-\mathrm{j}2\pi}{N}}$，即：列向量 $\boldsymbol{X}_0$ 的 4-WFRFT 可以通过矩阵 $\boldsymbol{F}_{4W}(\alpha,\boldsymbol{V})$ 得到。

WFRFT 的物理实现流程以及物理含义如图 1 所示，一个长度为 N 的信息序列经过串并转换后进入 4 个支路分别进行处理。其中，通过 w_1 和 w_3 支路的信号数据在经过加权处理之前都经过了 DFT 模块，因而 w_1 和 w_3 支路刚好对应于 OFDM 的多载波系统结构。而相对应的 w_0 和 w_2 支路，其过程中没有经过 DFT 模块，对应的则是单载波系统结构。

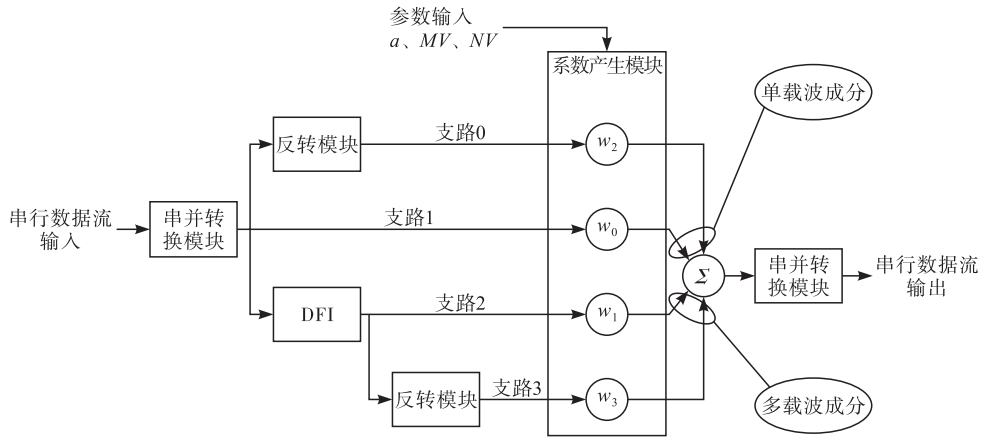

图 1　WFRFT 的物理实现流程

3　CR-WFRFT 物理层认证系统模型

本文提出一种将星座图旋转角度与 WFRFT 相结合的物理层认证方法，进一步提高认证过程中的安全性。

在加权系数的作用下，信号在复平面上展现的图样会随着 α 的递增呈现一种旋转的变化，同时在这一旋转过程中图样会出现扩散、拉伸等一系列附属变化，可将每个加权系数引起的旋转角度表示为：

$$\theta_l=\arctan\frac{\mathrm{Im}[w_l(\alpha)]}{\mathrm{Re}[w_l(\alpha)]}=$$
$$\arctan\frac{\pm\sin\left[\frac{3\pi(\alpha-1)}{4}\right]}{\cos\left[\frac{3\pi(\alpha-1)}{4}\right]}=\frac{\pm3\pi(\alpha-1)}{4},$$
$$(l=0,1,2,3) \tag{8}$$

通过确定 θ_l 可以决定图样在复平面上的旋转趋势，这一趋势同时反映了 4 个加权函数分量各自旋转效果的综合叠加。由于同一 α 下得到的 θ_l 一般不同，往往会造成 4 个分量之间的相对性旋转，进而导致图样在旋转过程中的多样变化。

通过仿真实验可以看出，随着参数 α 的逐步增大，原本重合在一起的 4 个基础星座点也逐步随之旋转散开，4 个基础星座点的相对界限也愈加模糊，参数 α 增大到一定程度后，会导致星座混叠在一起而无法区分。因此，引入 WFRFT 使星座充分混叠，通过提高星座图的整体复杂度的方法，可以使认证过程的安全性得到较好地提升。

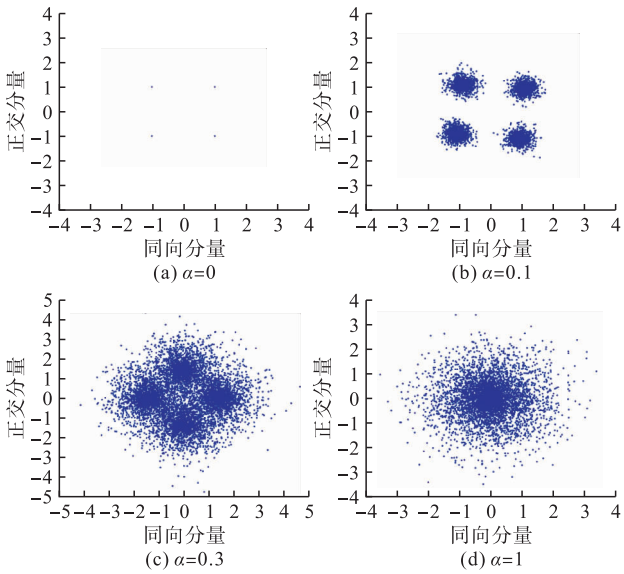

图 2　经过 WFRFT 的 QPSK 信号星座图

图 3 给出了 CR-WFRFT 物理层认证系统（之后简称 CR-WFRFT）传输结构模型，CR-WFRFT 的设计是为了提高物理层认证的复杂度与安全性，系统数据发送方与调制水印进行数字基带映射之后，利用 WFRFT 技术对带有认证标签的调制水印

进行处理,使其表现出之前不曾具备的高复杂度,以达到提高信号安全性的目的。

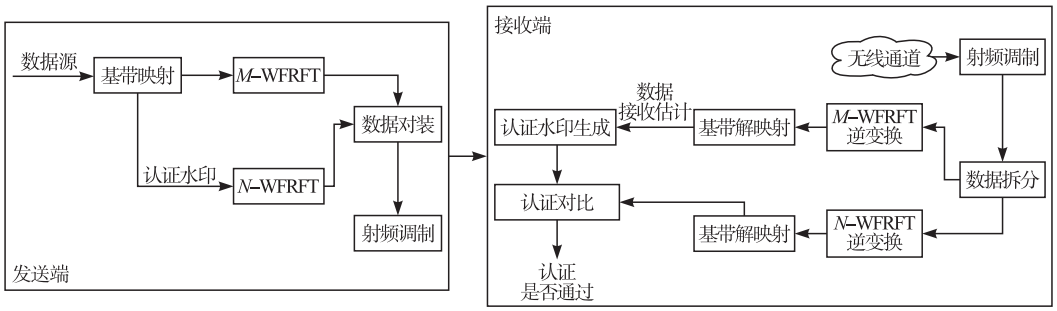

图 3 CR-WFRFT 系统流程图

如图 3 所示,用户数据比特序列 $\{d\}^M \in \{0,1\}$ 以及调制水印比特序列 $\{t\}^N \in \{0,1\}$ 分别被映射成为具有不同星座特征的符号序列 $\boldsymbol{D}=[D_0, D_1,\cdots,D_{M-1}]$ 以及 $\boldsymbol{T}=[T_0,T_1,\cdots,T_{N-1}]$,2 个符号序列经过 WFRFT 进行信号特征转化可以表示为:

$$x(t)=\sum_{p=1}^{M+N} S_p U(t)\psi(\theta(t),u,t),t\in[0,T_d] \tag{9}$$

式中:T_d 为数据分组的所持续时间;$U(t)$、$\theta(t)$ 为 WFRFT 控制函数。由于任意 WFRFT 的定义都来源于 4-WFRFT,因此可将 WFRFT 的核函数定义为:

$$\psi(\theta(t),u,t)=w_0(\theta(t)\delta(u-t))+\frac{1}{\sqrt{2\pi}}w_1(\theta(t))\exp(-\mathrm{j}ut)+w_2(\theta(t)\delta(t-u))+\frac{1}{\sqrt{2\pi}}w_3(\theta(t))\exp(\mathrm{j}ut) \tag{10}$$

为简化后续研究,将 CR-WFRFT 系统的传输过程看作 2 个独立的进程进行分析研究。在数据源传输过程中,用户数据符号序列 $\boldsymbol{D}=[D_0,D_1,\cdots,D_{M-1}]$ 以及调制水印符号序列 $\boldsymbol{T}=[T_0,T_1,\cdots,T_{N-1}]$ 分别经参数 α、β 的 4-WFRFT 处理:

$$\begin{cases}\boldsymbol{D}=w_0^{\alpha}D_m+w_1^{\alpha}\dfrac{1}{\sqrt{M}}\displaystyle\sum_{k=0}^{M-1}D_k\mathrm{e}^{-\mathrm{j}\frac{2\pi}{M}km}+\\ w_2^{\alpha}D_{(M-m)}+w_3^{\alpha}\dfrac{1}{\sqrt{M}}\displaystyle\sum_{k=0}^{M-1}D_k\mathrm{e}^{\mathrm{j}\frac{2\pi}{M}km}\\ \boldsymbol{T}=w_0^{\beta}T_n+w_1^{\beta}\dfrac{1}{\sqrt{N}}\displaystyle\sum_{k=0}^{N-1}T_k\mathrm{e}^{-\mathrm{j}\frac{2\pi}{N}kn}+\\ w_2^{\beta}T_{(N-n)}+w_3^{\beta}\dfrac{1}{\sqrt{N}}\displaystyle\sum_{k=0}^{N-1}T_k\mathrm{e}^{\mathrm{j}\frac{2\pi}{N}kn}\end{cases} \tag{11}$$

经过 CR-WFRFT 系统的处理过后,用户数据符号序列 $\boldsymbol{D}=[D_0,D_1,\cdots,D_{M-1}]$ 及调制水印符号序列 $\boldsymbol{T}=[T_0,T_1,\cdots,T_{N-1}]$ 均在信号特征方面表现出了与之前的不同,由于 WFRFT 技术的多样选择变换性,使得 CR-WFRFT 系统本身具备了较强的灵活性。

信号接收端对认证水印的数据恢复过程可表示为:

$$T=w_0^{(-\beta)}T_n+w_1^{(-\beta)}\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}T_k\mathrm{e}^{-\mathrm{j}\frac{2\pi}{N}kn}+w_2^{(-\beta)}T_{(N-n)}+w_3^{(-\beta)}\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}T_k\mathrm{e}^{\mathrm{j}\frac{2\pi}{N}kn} \tag{12}$$

同时根据 WFRFT 的可逆性原则,式(11)、(12)中的加权系数 $\{w_p^{(-\beta)}\}_{p=0}^3$ 以及 $\{w_p^{\beta}\}_{p=0}^3$ 将遵循如式(13)所示的约束条件:

$$\begin{cases}w_0^{(-\beta)}w_0^{\beta}+w_1^{(-\beta)}w_3^{\beta}+w_2^{(-\beta)}w_2^{\beta}+w_3^{(-\beta)}w_1^{\beta}=1\\ w_0^{(-\beta)}w_1^{\beta}+w_1^{(-\beta)}w_0^{\beta}+w_2^{(-\beta)}w_3^{\beta}+w_3^{(-\beta)}w_2^{\beta}=0\\ w_0^{(-\beta)}w_2^{\beta}+w_1^{(-\beta)}w_1^{\beta}+w_2^{(-\beta)}w_0^{\beta}+w_3^{(-\beta)}w_3^{\beta}=0\\ w_0^{(-\beta)}w_3^{\beta}+w_1^{(-\beta)}w_2^{\beta}+w_2^{(-\beta)}w_1^{\beta}+w_3^{(-\beta)}w_0^{\beta}=0\end{cases} \tag{13}$$

同时,在研究用户数据序列时,由于所采取的认证水印源自于信号自身的星座图旋转状态,因此不会对信号传输以及接收端解码造成任何影响。

3 系统性能仿真与分析

本文信道环境设定为瑞利信道,且假设信道为理想估计,发射端功率受限。为有助于分析结果,基带映射采用 QPSK 映射。

信号特征作为窃听方窃听数据的重要依据,也作为物理层认证的关键,是认证过程中最需要注意的部分。图 4 为 CR-WFRFT 系统被在基于高阶累积量的识别方法时的识别概率曲线,从信号识别过程来看,随着信噪比不断增大,传统 QPSK 的信号识别概率呈稳步上升趋势,并在最终会达到 100%。而采用 WFRFT-QPSK 方式的信号初始识别率偏高,随着信噪比增大呈下降趋势。这是由于信噪比较低时,噪声占据信号主体部分,其随机性使得 CR-WFRFT 的信号输出存在较大的波动,在仿真结果中呈现出较高的识别概率。而随着信噪比的增大主体呈下降趋势,并在最终无限趋近于 0。仿真结果在一定程度上表明:CR-WFRFT 系统拥有相较传统通信方式更低的被识别概率,体现出了 CR-

WFRFT 系统在基于高阶累积量识别方法中的优越性。

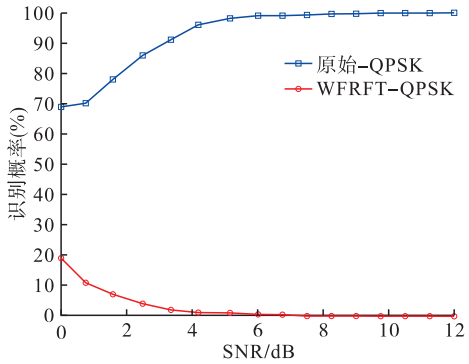

图 4　CR-WFRFT 系统被识别性能分析

根据图 5 可以看出，虽然 CR-WFRFT 解调方式与 QPSK 理论值仍有细微差距，但已无限接近理论误码率曲线，而与传统 QPSK 解调存在较大偏差。这就表明 CR-WFRFT 不会影响信号接收端在信号传输过程中数据的精确性，同时也表明了 CR-WFRFT 信号对传统解调方式具备一定的抵抗性，无论信号特征的如何变化，传统解调方式都无法从中获取有效信息。传统解调方式的失效无疑提高了在物理层认证过程中的安全性。

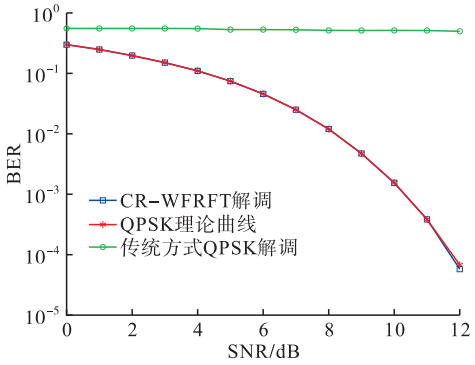

图 5　CR-WFRFT 系统误码性能分析

5　结语

本文提出了一种 WFRFT 与星座图旋转相结合的物理层认证方法，星座图旋转角度可作为水印信息嵌入基带信号当中，而不影响信号的正常传输，WFRFT 则利用高复杂性将星座充分混叠，必需经过相应的逆变换才能正确解调信息，极大地提高了认证过程的安全性。

参考文献

[1] KOHNO T, BROIDO A, CLAFFY K C. Remote Physical Device Fingerprinting[J]. 2005 IEEE Transaction on Security and Privacy, 2005, 2(2):93-108.

[2] DANEB B, CAPKUN S. Transient-Based Edentification of Wireless Sensor Nodes[C]//International Conference on Information Processing in Sensor Networks. San Francisco, CA, USA: IEEE, 2009: 25-36.

[3] DANEV B, ZANETTI D, CAPKUN S. On Physical-Layer Identification of Wireless Devices[J]. ACM Computing Survey, 2012, 45(1): 1-29.

[4] YU P L, BARAS J S, SADLER B M. Physical Layer Authentication [J]. IEEE Transactions on Information Forensics & Security, 2008, 3(1):38-51.

[5] WEN H, HO P H, GONG G. A Novel Framework for Message Authentication in Vehicular Communication Networks[C]//Proceedings of Global Telecommunications Conference. Honolulu, HI, USA:IEEE, 2009: 1-6.

[6] WEN H, WANG Y, ZHU X, et al. Physical Layer Assist Authentication Technique for Smart Meter System[J]. IET Communications, 2013, 7(7): 189-197.

[7] WEN H. Physical Layer Assisted Authentication for Wireless Sensor Networks[J]. IET Information Security, 2011, 4(4): 390-396.

[8] WEN H, HO P H. Physical Layer Technique to Assist Authentication Based on PKI for Vehicular Communication Networks[J]. KSII Transactions on Internet & Information Systems, 2011, 5(2):440-456.

[9] ZHANG J, WEN H, SONG H, et al. Using Basis Expansion Model for Physical Layer Authentication in Time-Variant System [C]//IEEE Communications and Network Security (CNS). Philadelphia, PA, USA:IEEE, 2016:348-349.

[10] XIAO L, GREENSTEIN L J, MANDAYAM N B, et al. Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication[C]//IEEE International Conference on Communications. Glasgow, UK:IEEE, 2007:4646-4651.

[11] SHANG D, ZENG K, XIANG W, et al. PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9):1817-1827.

[12] FANG X J, ZHANG N, ZHANG S, et al. On Physical Layer Security: Weighted Fractional Fourier Transform Based User Cooperation[J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5498-5510.

[13] FANG X J, SHA X J, LI Y. Secret Communication Using Parallel Combinatory Spreading WFRFT[J]. IEEE Communications Letters, 2015, 19(1): 62-65.

[14] FANG X J, SHA X J, MEI L, Guaranteeing Wireless Communication Secrecy via a WFRFT Based Cooperative System[J]. China Communications, 2015,

12(9): 62-6576-82.

[15] FANG X J. SHA X J, LI Y. MP-WFRFT and Constellation Scrambling Based Physical Layer Security System[J]. China Communications, 2016, 13(2): 138-145.

[16] FANG X J, SHA X J, ZHANG N. et al. Towards PHY-Aided Authentication via Weighted Fractional Fourier Transform [C]// 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). Montreal, Canada:IEEE, 2016:1-5.

[17] FANG X J, WU X L, ZHANG N, et al. Safeguarding Physical Layer Security Using Weighted Fractional Fourier Transform[C]//2016 IEEE Global Communications Conference(GLOBECOM). Washington DC,USA:IEEE, 2016: 1-6.

[18] FANG X J, ZHANG N, SHA X J, et al. Physical Layer Security: a WFRFT-Based Cooperation Approach[C]// 2017 IEEE International Conference on Communications (ICC). Paris, France:IEEE, 2017: 21-25.

[19] 达新宇,翟东,梁源,等.联合多层 WFRFT 与人工噪声的抗截获通信技术[J].华中科技大学学报(自然科学版),2018,46(10):86-91.

[20] 宋华伟,金梁,王旭.无线网络物理层安全认证方法[J].西安交通大学学报,2018,52(4):105-110,138.

[21] 王旭,金梁,黄开枝.基于物理层位置信息的跨层双向认证[J].信息工程大学学报,2017,18(3):279-283,304.

(编辑:徐楠楠)

(上接第 92 页)

[5] 刘丹军, 蔡桂林, 王宝生. AMTD:一种适应性动态目标防御方法[J]. 网络与信息安全学报, 2018, 4(1):1-12.

[6] 周余阳, 程光, 郭春生. 基于贝叶斯攻击图的网络攻击面风险评估方法[J]. 网络与信息安全学报, 2018, 4(6): 11-22.

[7] JIN H P, SHAILENDRA R, DAESUNG M, et al. MTD-Spamguard: a Moving Target Defense-Based Spammer Detection System in Social Network[J]. Soft Computing, 2018, 22 (20): 6683-6691.

[8] VAHID Z, MEHDI S. A Cost-Sensitive Move Selection Strategy for Moving Target Defense[J]. Computers & Security, 2018, 75:72-91.

[9] 张恒巍,余定坤,韩继红. 基于攻防信号博弈模型的防御策略选取方法[J].通信学报,2016,37(5):51-61.

[10] 张恒巍,李涛. 基于多阶段攻防信号博弈的最优主动防御[J].电子学报,2017,45(2):431-439.

[11] 张恒巍, 李涛, 黄世锐. 基于攻防微分博弈的网络安全防御决策方法[J]. 电子学报, 2018, 424(6): 151-158.

[12] 陈子涵, 程光. 基于 Stackelberg-Markov 非对等三方博弈模型的移动目标防御技术[J]. 计算机学报, 2020,43(3):512-525.

[13] TAN J L, LEI C, ZHANG H Q, et al. Optimal Strategy Selection Approach to Moving Target Defense Based on Markov Robust Game[J]. Computers & Security, 2019, 85:62-76.

[14] 姜伟, 方滨兴, 田志宏. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2013, 47(10): 1714-1723.

[15] 黄健明, 张恒巍, 王晋东, 等. 基于攻防演化博弈模型的防御策略选取方法[J]. 通信学报, 2017, 38(1): 168-176.

[16] 李艳, 黄光球, 张斌. 动态攻击网络 Markov 演化博弈安全分析模型[J]. 计算机科学与探索, 2016, 10(9): 1272-1281.

[17] 张恒巍, 黄健明. 基于 Markov 演化博弈的网络防御策略选取方法[J]. 电子学报, 2018, 46(6): 1503-1509.

[18] 黄健明, 张恒巍. 基于随机演化博弈模型的网络防御策略选取方法[J]. 电子学报, 2018, 46(9): 2222-2228.

[19] 马润年, 陈彤睿, 王刚, 等. 面向隔离区异构平台的动态防御主动迁移策略[J]. 火力与指挥控制, 2019, 44(3): 1-8,22.

[20] 国家信息安全漏洞库. 漏洞信息[EB/OL]. [2018-11-3]. http: //www. cnnvd. org. cn .

[21] National Vulnerability Database. Common Vulnerabilities and Exposures[EB/OL]. [2018-11-03]. https://nvd. nist. gov.

[22] 高妮, 高岭, 贺毅岳, 等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报(工程科学版), 2016, 48(1): 111-118.

(编辑:徐敏)